内蒙古自治区中等职业教育规划教材
中等职业教育课程改革实验教材

计算机网络技术与应用（第2版）

史秀峰　葛宗占　主　编

侯塞平　管志宇　副主编

電子工業出版社
Publishing House of Electronics Industry
北京・BEIJING

内 容 简 介

本书内容包括计算机网络概述、数据通信基础、计算机网络体系结构、局域网技术、网络管理与安全、交换与路由技术和综合实训等内容。在教材的编写中注重反映新知识、新技术、新方法，体现科学性、实用性。正确处理了理论知识和技能实践的关系，注重培养学生的分析能力、应用能力和自学能力。

本书内容丰富、结构清晰，适合作为中等职业学校计算机应用专业的课程教材，以及供广大计算机爱好者参考使用。

图书在版编目（CIP）数据

计算机网络技术与应用 / 史秀峰，葛宗占主编．—2 版．—北京：电子工业出版社，2016.8
内蒙古自治区中等职业教育规划教材　中等职业教育课程改革实验教材

ISBN 978-7-121-28101-3

Ⅰ．①计… Ⅱ．①史… ②葛… Ⅲ．①计算机网络—中等专业学校－教材 Ⅳ．①TP393

中国版本图书馆 CIP 数据核字（2016）第 020436 号

策划编辑：关雅莉
责任编辑：柴　灿　　文字编辑：张　广
印　　刷：
装　　订：
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1 092　1/16　印张：13.75　字数：352 千字
版　　次：2013 年 1 月第 1 版
　　2016 年 8 月第 2 版
印　　次：2016 年 8 月第 1 次印刷
定　　价：29.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：（010）88254617，Luomn@phei.com.cn。

前言

随着计算机技术的发展，中职教育计算机专业的多数课程已经不能满足社会的需要。根据国家新一轮课程改革的精神和中等职业学校计算机专业发展的需要，2012 年在内蒙古教育厅的组织下召开了计算机专业教材编写、修订会议。这次会议对计算机专业教材编写提出了新的要求，即：以充分适应本专业最新发展趋势为原则，培养学生的从业能力，为就业及进入更高层次的学习奠定良好的基础。为此我们特地重新规划了计算机专业的教学计划和课程安排，力求新教材能更加适应社会的发展，同时在众多本专业课程中选出了《计算机网络技术与应用》、《计算机组装与维修》、《Office 2007 案例教程》、《Visual Basic 语言程序设计》4 门基础性强的课程作为自 2015 年始的中职对口升入高等院校计算机专业的必考课程。

为了方便广大中等职业学校的学生学习，我们特别组织编写了相应的学习指导书。它们是《计算机网络技术与应用学习指导与练习》、《计算机组装与维修学习指导与练习》、《Office 2007 案例教程学习指导与练习》、《Visual Basic 语言程序设计学习指导与练习》。

按照新的教学计划和课程安排，我们将所有教材纳入《内蒙古自治区中等职业教育规划教材·中等职业教育课程改革实验教材》丛书体系。本套教材由葛宗占任总编，负责组织在教学一线的骨干教师编写。

本书是对已出版的《计算机网络技术与应用》一书的修订，由史秀峰、葛宗占担任主编，侯塞平、菅志宇担任副主编，参加编写的人员还有赵鹏飞、李宇民、吕红宇、杨延青。

虽在编写中力求谨慎，但限于编者的学识、经验，疏漏和不足之处仍恐难免，恳请广大同行和读者不吝赐教，以便今后修改提高。

编　者

2016 年 7 月

目录

第 1 章 计算机网络概述

内容摘要

- 计算机网络的产生与发展
- 计算机网络的概念
- 计算机网络的功能
- 计算机网络的分类
- 计算机网络系统的拓扑结构
- 计算机网络的标准及标准化组织

学习目标

- 了解计算机网络产生与发展的过程
- 理解计算机网络的概念
- 掌握计算机网络的功能
- 掌握计算机网络的分类
- 理解计算机网络系统的拓扑结构
- 熟悉有影响的标准化组织

计算机网络是计算机技术与通信技术紧密结合的产物，是现代信息社会的基础设施。连接各个部门、地区、国家乃至全世界的计算机网络可以使人们获取、传输、处理和存储信息，帮助我们进行生产的控制、企业的管理甚至国家政策的制定。随着计算机网络技术的不断更新，计算机网络的应用已经渗透到各行各业乃至家庭，并逐步改变着人们的思想观念、工作模式和生活模式，成为人们日常生活中不可或缺的工具。

现代信息社会带给人们许许多多的便利条件，如每天的新闻、天气预报、教育、医疗、网上办公、网上缴费、网上银行等各种各样的网络应用。自从有了计算机网络，人们的生产、生活的方式都发生了巨大的变化，可以说计算机网络已经在各个方面影响并改变着人们的生活。

1.1 计算机网络的产生与发展

计算机网络技术是计算机及其应用技术和现代通信技术密切结合的产物，是随着社会对信息资源的共享和信息传递的要求而发展起来的。

早期的每台计算机都独立于其他计算机，它们自行工作，具有的资源也只能自己享用。现在，计算机网络是将分布在不同地理范围内的、具有独立功能的计算机系统及其外部通信设备，通过通信线路连接起来，并在网络操作系统、网络管理软件及网络通信协议的管理和协调下，实现彼此资源共享、信息传递、协同工作和在线处理等功能的系统。如图 1-1 所示为典型的计算机网络系统。

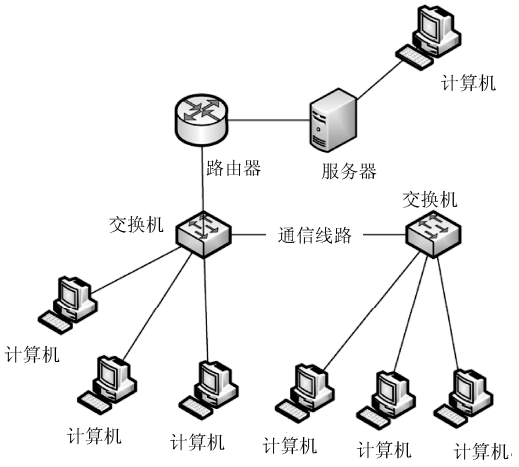


图 1-1　计算机网络系统

1.1.1 计算机网络的发展简史

随着计算机技术和通信技术的不断发展，计算机网络也随之经历了不同的发展时期。其发展历史包括从简单到复杂、从单机到多机的过程，一般可以划分为以下 4 个阶段。

1．具有通信功能的终端——第一代计算机网络

20 世纪 60 年代初期是计算机网络发展的萌芽阶段，该阶段的计算机通信系统被称为联机系统。联机系统是指以一台中央主计算机连接不同地理位置的多个终端。其中，终端是指一台计算机的外部设备，包括显示器和键盘，如图 1-2 所示是具有通信功能的终端系统。通常将该阶段的系统称为面向终端的计算机网络。

第一代计算机网络的特征是多台终端能够以交互的方式将命令发送至计算机，从而将一台计算机内的各种资源分配给多个用户共同使用，提高计算机的利用率。这种方式使得人们能够以较低的费用使用昂贵的计算机，从而极大地刺激了用户使用计算机的热情，使

计算机用户的数量迅速增加。这种网络形式的典型例子是美国航空公司第一个联机预定飞机票的 SADREI 实时系统，它用一台中心计算机与全美 2000 个终端机相连。

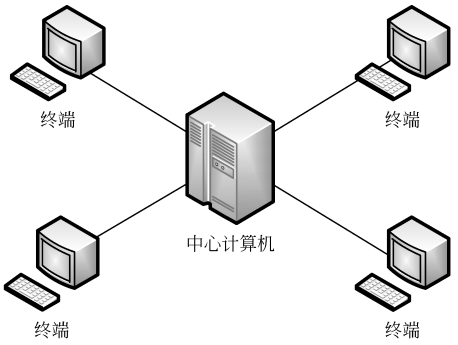


图 1-2　具有通信功能的终端系统

但是，随着终端用户的不断增多，也加重了中心计算机的负担，使得系统响应时间过长，严重时甚至出现死机等负面影响。而且，一旦中心计算机出现故障，将导致整个计算机网络系统瘫痪。

2．发展完善阶段——第二代计算机网络

随着第一代计算机网络的发展，人们于 20 世纪 60 年代中期开始研究将多台计算机相互连接的方法。最具代表性的是 1969 年由美国国防部高级研究计划局（DARPA）建成的 ARPANET 实验网。最初的 ARPANET 只有 4 个节点，它以电话线路作为主干网络，从而形成了早期的计算机网络，其网络结构如图 1-3 所示。

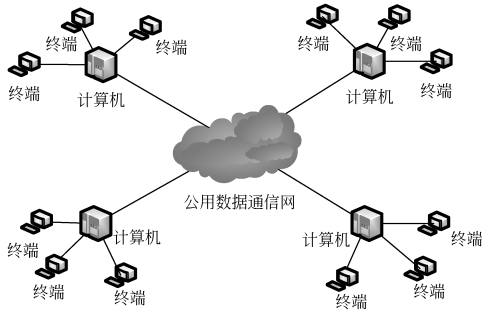


图 1-3　ARPANET 结构示意图

ARPANET 包括资源共享、分散控制、分组交换、专门的通信控制处理机、分层的网络协议等特点。其特点也正是现在计算机网络的基本特征。

到了 20 世纪 70 年代中后期，广域通信网迅速发展，各发达国家的政府部门、研究机构和各大计算机公司都在发展分组交换网络。这些网络实现了计算机之间的远程数据传输及共享，通信线路大多采用租用电话线路。但这些网络也存在不少弊端，其主要问题在于不同厂家提供的网络产品难以实现统一，甚至无法互联，各自有着不同的网络体系。

3．互联互通阶段——第三代计算机网络

由于第二代计算机网络没有统一的计算机网络标准，其普及程度非常低。因此，计算机网络走向体系结构标准化变得十分必要和紧迫。在这种形势的发展下，1984 年国际标准化组织（ISO）正式颁布了一个网络体系结构的国际标准——开放系统互联参考模型（OSI/RM）。

OSI/RM 即 Open System Interconnection/Reference Model（开放系统互联参考模型）的缩写。它是一种概念上的网络模型，其作用是规定了网络体系结构的框架，保证了不同网络设备间的兼容性和互操作性。

20 世纪 80 年代，随着微型计算机的广泛应用，将小范围内的多台计算机互联以达到资源共享的需求日益增加。例如，为使校园内的多台计算机能够共享资源，或让实验室内的所有计算机能够与外部计算机共同完成科学项目，部分研究所和大学开始致力于对局域网的研究。1980 年 2 月，在旧金山成立的国际电子电气工程师协会（IEEE）也在 OSI/RM 标准的基础上制定了 IEEE 802 局域网标准，为随后计算机局域网络技术的规范化发展打下了坚实的基础。如图 1-4 所示为第三代计算机网络结构示意图。

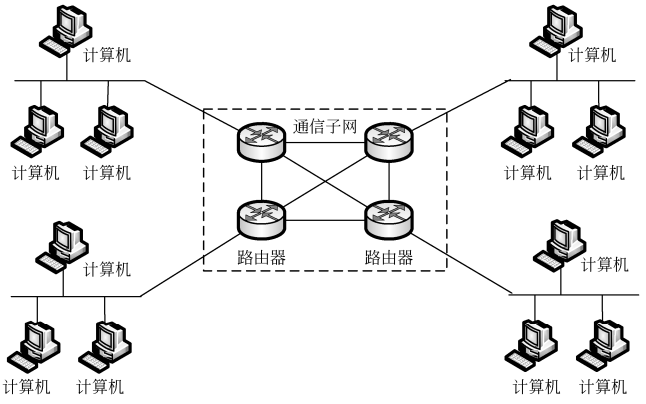


图 1-4　第三代计算机网络结构示意图

4．飞速发展阶段——第四代计算机网络

第四代计算机网络的特征是以 Internet 为主体的高速、智能化互联网络飞速发展。经过几十年的发展，计算机网络凸显出它的使用价值和良好的应用前景。进入 20 世纪 90 年代后，特别是 1993 年美国宣布建立国家信息基础设施（National Information Infrastructure，NII）后，许多国家纷纷制定及建立符合本国需要的 NII，这不仅极大地推动了计算机网络技术的发展，也促使计算机网络进入高速发展阶段。如图 1-5 所示为第四代计算机网络结构示意图。

目前，计算机网络正朝着高速化、实时化、智能化、集成化和多媒体化的方向不断深入发展，全球以 Internet 为核心的高速计算机互联网络已经形成，Internet 已经成为人们最重要的、最大的知识宝库。

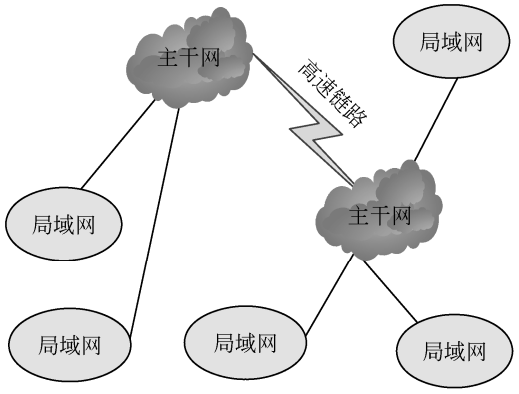


图 1-5　第四代计算机网络结构示意图

参考链接

我国计算机网络的发展:

（1）铁道部于 1980 年开始联网实验。

（2）1987 年 9 月 20 日北京计算机技术研究所的钱天白教授发出第一封 E-mail，标志着 Internet 已经成为中国人生活的一部分，揭开了 Internet 在我国发展的序幕。

（3）1989 年 2 月我国的第一个公用分组交换网 CHINAPAC 通过试运行和验收，达到了开通业务的条件。

（4）1993 年底国家有关部门决定兴建“金桥”、“金卡”、“金关”工程，简称“三金”工程。

（5）从 1994 年开始，我国建成四大互联网，即中国科学技术网（CSTNET）、中国教育和科研计算机网（CERNET）、中国公用计算机互联网（CHINANET）和中国金桥信息网（CHINAGBN）。

1.1.2 计算机网络的发展趋势

计算机网络正在向综合化、智能化、高速化发展，从计算机网络应用来看，网络应用系统将向更深和更宽的方向发展。首先，Internet 信息服务将会得到更大发展。网上信息浏览、信息交换、资源共享等技术将进一步提高速度、容量及信息的安全性。其次，远程会议、远程教学、远程医疗、远程购物等应用已逐渐成为了现实。物联网、云计算、虚拟现实技术的应用也成为网络发展的热门技术。

美国政府 1993 年提出的“信息高速公路”计划不仅推动了互联网本身的发展，也促进了对下一代互联网的研究。2002 年，各国发起“全球高速互联网 GTRN”计划，积极推动下一代互联网技术的研究和开发。与现在使用的互联网相比，下一代互联网有以下不同：

（1）更大。由于现有 IPv4 地址将在近年迅速耗尽，世界互联网发展将受严重限制。下一代互联网将逐渐放弃 IPv4 地址协议，启用新版 IPv6 地址协议，IP 地址的数量将从 2 的 32 次方增加到 2 的 128 次方，地址资源极为丰富，有人形容世界上每一粒沙子都会有一个

IP 地址。网络规模将更大，接入网络的终端种类和数量更多，网络应用更广泛。

（2）更快。在下一代互联网，高速强调的是端到端的绝对速度，至少 100Mbps。至于能高到什么程度，这有赖于传输技术的不断发展。2004 年 12 月 7 日，CERNET 在北京与天津之间就实现了世界上第一次有真实流量的 40Gbps 互联带宽。

（3）更安全。目前的计算机网络因为种种原因，在体系设计上有一些不够完善的地方，下一代互联网将在建设之初就从体系设计上充分考虑安全问题，使网络安全的可控性、可管理性大大增强。

基于以上特点，未来的互联网将更方便、更及时，真正的数字化生活即将来临。可以用任何一种方式高速上网，任何可能的东西都会成为网络化生活的一部分。

1.2 计算机网络的基本概念

从计算机网络的发展过程我们可以看出，从 20 世纪 50 年代到现在，在短短几十年的时间中，从最早只能互通的单机系统到现在互联、互通、高速、智能化的计算机网络，从早期只有专业人员才能使用的昂贵系统到现在普通人生活的方方面面不可或缺的组成部分，计算机网络在形式、内容、组成上伴随着技术的不断进步而发生着变化。

1.2.1 计算机网络的定义

计算机网络是利用通信设备和线路，将处在不同地理位置、操作相对独立的多台计算机设备连接起来，再配置一定的操作系统和应用软件，实现计算机软硬件资源共享及信息传递的系统。

计算机网络具有如下特征。

（1）计算机设备间需要用通信设备和传输介质互联。

（2）计算机设备间使用统一的规则即“网络协议”来交换信息。

（3）以实现资源共享和数据通信为主要目的。

1.2.2 计算机网络的构成

计算机网络是利用通信设备和网络软件，把地理位置分散而功能独立的多个计算机（及其智能设备）以相互共享资源和进行信息传递为目的连接起来的一个系统。

通俗地讲，计算机网络就是由多台计算机（或其他网络设备）通过传输介质和软件连接在一起组成的。这里的传输介质指的是一些通信设备及线路。“连接”意味着计算机之间可以互相传输数据、交换信息，如图像、文件。同时，这些计算机彼此之间也是平等的，任何一台计算机都不能干预其他计算机的工作，如启动、关闭。

由此可见，计算机网络与计算机系统类似，也是由硬件系统与软件系统构成的，只是计算机网络的硬件系统与软件系统都和通信密不可分。

从系统功能角度来看，计算机网络由资源子网和通信子网两个部分组成。通信子网一般由通信设备、网络介质等物理设备所构成，提供网络通信功能；资源子网是网络中实现资源共享的设备和软件的集合，主要负责全网的信息处理，为用户提供各种网络资源及网络服务。

对局域网来说，通信子网由网卡、线缆、中继器、网桥、路由器、交换机等设备和相关软件（如协议）组成。资源子网由联网的服务器、工作站、共享打印机等相关设备和网络操作系统、网络应用软件等组成。

综上所述，组成一个网络必须具备三个条件：

（1）两台或两台以上具有独立工作能力的计算机，用来提供或使用服务。

（2）通信子网：由传输介质和通信设备组成。

（3）网络软件：网络操作系统、网络应用软件以及一系列实现网络传输的网络通信协议（网络通信协议：为确保网络中的计算机相互之间能交换信息而建立的规则、标准或约定。例如，TCP/IP 是目前互联网使用的用于网络互联的通信协议）。

1.2.3 计算机网络的功能

计算机网络在整个社会经济发展、娱乐休闲、科技教育等方面都发挥着积极的作用。归纳起来，计算机网络的功能可以包含以下几个方面。

1．资源共享

“资源”是指计算机网络中所有的软件、硬件和数据资源。“共享”是指计算机网络中的用户都能够部分或全部的享受这些资源，其中，部分或全部共享是由于受经济和其他因素的制约而决定的，但并不是所有的用户都能够独立拥有这些资源。硬件资源共享最典型的例子就是打印机通过共享，使网络中多用户共用一台打印机进行文件打印；软件资源共享常见的例子就是从网络上下载各种软件；数据资源共享的典型例子是数据库共享，如打开 QQ 软件时自动从 ISP（Internet 服务商）服务器获取好友名单。

计算机网络的资源共享使得普通用户能够共享网络中分散在不同地理范围内的各种软件、硬件资源，如大容量硬盘和打印机等资源，极大地提高了计算机软件、硬件的利用率，不仅方便了网络用户，而且节约了经济投资。

2．数据通信

计算机网络的基本功能之一就是计算机与计算机之间能够快速可靠地相互传递信息。这不局限于一个小的网络范围，而在一个覆盖范围很大的网络中，即使是相隔很远甚至不在相同国家的计算机用户之间也能够相互交换信息。例如，通过 Internet 世界各地的用户都能够实现彼此间通信。

3．负载均衡

负载均衡是指工作被均匀地分配给网络中的各台计算机进行处理，这样就减轻了单台计算机的工作负荷，提高了工作效率。负载均衡主要应用于服务器集群系统中，网络控制

中心负责分配和检测，当某台计算机的任务过重时，系统会通过网络将部分工作转交给较“空闲”的计算机去处理，使资源得到合理调整。

4．分布式处理

分布式处理也可以认为是一种并行处理形式。分布式处理系统将不同地点的，或具有不同功能的，或拥有不同数据的多台计算机用通信网络连接起来，在控制系统的统一管理控制下，协调地完成信息处理任务。例如一个综合性的大型课题，可以采用合适的算法将课题分为许许多多的小课题，分散到网络中不同的计算机上进行处理，然后再集中起来，使问题得到快速而经济的解决。

5．提高计算机的可靠性

在计算机网络中，当网络内的某一设备（通信线路或计算机等）发生故障时，可利用其他设备来完成数据的传输或将数据复制到其他系统内代为处理，以保证用户的正常操作。例如，当数据库内的信息丢失或遭到破坏时，可调用另一台计算机内备份的数据库来完成数据处理工作，并恢复遭到破坏的数据库，从而提高系统的可靠性和可用性。

1.2.4 计算机网络的类型

计算机网络的种类繁多、性能各异，根据不同的划分原则，可以分为各种不同类型的计算机网络。下面从几个不同的角度对计算机网络的类型予以介绍。

1．按网络的覆盖范围进行分类

虽然计算机网络类型的划分标准各种各样，但是按地理覆盖范围划分是一种大家都认可的通用网络划分标准，它可以很好地反映不同类型网络的技术特征。

按地理分布范围不同，可以将网络划分为局域网、城域网和广域网三种类型。

（1）局域网

局域网（Local Area Network，LAN）是限定在一定地理区域内（例如一幢大楼、一所学校、一个小区）的网络，其覆盖范围一般在几十千米以内，由互连的计算机、打印机、网络连接设备和其他在短距离间共享硬件、软件资源的设备组成。局域网数据传输速度快、可靠性高、误码率低，通常归属某个单一组织，由该组织维护和管理。

（2）城域网

城域网（Metropolitan Area Network，MAN）的规模介于局域网与广域网之间，地理范围从几十千米到上百千米，一般指覆盖一座城市的网络，主要用于政府机构和商业网络。城域网比局域网的连接距离更远，连接的计算机数目更多，从某种程度上说可以认为是局域网在地理范围上的延伸。

其设计目的是要满足几十千米范围内的大量企业、机关与社会服务部门的计算机连网需求。它是以光缆通信设施为基础，实现语音、数据、图像和视频等多种信息高速传输的综合信息网络。例如大型企业集团、电信部门、有线电视台和政府构建的专用网络和公用网络。

（3）广域网

广域网（Wide Area Network，WAN）也称远程网，覆盖范围通常为数百千米到数千千米，甚至数万千米，可以是一个地区或一个国家，甚至世界几大洲或整个地球。目前应用和连接范围最广的因特网（Internet）从网络技术角度来看就属于广域网的范畴，当然广域网不仅限于因特网，分布在不同城市，甚至不同国家的公司网络互联后形成的网络也属于广域网。

由于广域网地理位置分布广，使得单独建设一个广域网的成本非常昂贵，所以通常使用电信部门或其他提供通信服务的经营部门建设的传统公共传输网络来实现数据传输，并由其管理和控制。由于传输介质复杂（例如卫星、电话线等），传输距离远，数据的传输速率较低，且误码率较高。

广域网主要作用是提供公共服务，不过也有专用服务的，例如某大型集团公司分布在各地的多家分支机构、合作伙伴和供应商的网络互联后形成的大型网络。

2．按照网络的管理方式分类

（1）对等网

对等网通常是由很少几台计算机组成的网络。采用分散管理的方式，网络中的每台计算机既作为客户机又作为服务器，每个用户都管理自己机器上的资源，所有的主机在网络上处于一种对等的地位。

（2）客户机/服务器网络

客户机/服务器网络，常称为 C/S 网络。它的管理工作集中在运行特殊网络操作系统与服务器软件的计算机上进行，这台计算机被称为服务器。服务器可以验证登录网络用户的用户名和密码的相关信息，处理客户机的请求，为客户机执行数据处理任务和提供信息服务。

3．按网络传输介质进行分类

按网络传输介质的不同将网络分为有线网络和无线网络。

（1）有线网络

有线网络是采用看得见、摸得着的线缆（同轴电缆、双绞线、光纤等）作为传输介质，将计算机以及相关设备进行连接，以实现计算机之间数据通信的网络。目前，绝大多数网络都是有线网络。

有线网络有以下优点。

① 工程造价低：实现方法较为简单，网络设备价格相对较低。

② 传输速率高：普通五类双绞线可以提供 100Mbps 或 1000Mbps 的传输速率，光纤的传输速率可以达到 10Gbps。而目前无线网络的传输速率约在 300Mbps 左右，但在实际使用中，多种因素会使传输速率受到很大的影响。

③ 传输距离远：无线局域网在室内的有效传输距离只有 100m，在室外可达 300m。而单模光纤的传输距离可达 100km，且传输速率可达 1000Mbps。

④ 受外界干扰小：无线网络随外界干扰强度和传输距离的增加，无线网络所提供的通信速率也会越来越低，直至无法通信。光纤则不受外界电磁信号的影响，传输速率和传输

距离都不会因此而改变。

（2）无线网络

无线网络（WLAN）就是采用无线通信技术实现数据传输的网络，与有线网络最大的区别在于传输介质的不同，它是利用空间电磁波代替传统电缆，提供传统有线网络的功能。无线网络作为一种简单、便捷的接入方式，随着其成本的不断下降，越来越受到人们的青睐。

无线网络拥有以下优点。

① 部署灵活：对于无线网络避免了有线网络施工的诸多障碍，只需安装天线即可。利用网络设备还可以将无线网络与有线网络无缝集成。

② 建设速度快：无线网络安装的主要工作是架设天线和安装联网设备，由于无线设备集成化程度高，安装所需工程量较小。

③ 安全性好：有线网络使用的线缆容易发生故障，安全性相对差。无线抗灾能力强，可以在很大程度上提高网络的安全性。

4．按网络使用的传输技术分类

根据网络中数据传输的方式可分为广播式传输网络和点对点传输网络。

（1）广播式传输网络

网络中的所有节点通过一条共享的通信介质连接起来，任意一个节点发送信息时，网络中所有节点都将会接收并处理这个信息。由于发送的信息中带有目的地址与源地址，接收到该信息的节点将检查目的地址是否与本节点的地址相同。如果相同，则接受该信息，否则将丢弃。

但是如果一个广播域中的节点数量过多，任何主机发送的广播都会扩散到整个区域，会引起广播泛滥，影响正常网络通信。广播技术很好地解决了传输介质共享的问题，降低了组网的成本和难度，总线型网络就是典型的广播式网络。

（2）点对点传输网络

点对点网络由许多互相连接的节点构成，节点之间都存在一条通信信道，数据以点到点的方式在网络中传输，可独占通信信道，能够获得高速率，高可靠性和稳定的延迟。当一台计算机发送数据分组后，它会根据目的地址，经过一系列的中间设备的转发，直至到达目的节点。如星型和网状型网络采用的就是点对点传输形式。

1.3　计算机网络的拓扑结构

联网的计算机之所以能与网络上的其他计算机通信，是因为该计算机与网络上的其他计算机具有物理上（或逻辑上）直接或间接的连接，不同的连接方式形成不同的计算机网络结构，也决定计算机网络使用不同的联网技术。

组建计算机网络时，第一个步骤就是拓扑结构的设计，它对网络的性能、可靠性与通信费用都有较大影响。

1.3.1 拓扑结构的概念

在研究计算机网络组成结构的时候，可以采用拓扑学中一种研究与大小形状无关的点、线特性的方法，即把工作站、服务器等网络设备抽象为“节点”，把网络中的电缆等通信介质抽象为“线”，这样隐去了网络的具体物理特性（如距离、位置等）而抽象出节点之间的关系加以研究。

从拓扑学的观点来看，计算机网络的拓扑结构，即是指网络中计算机或设备与传输介质形成的节点与通信线路间的几何排序，用以表示网络的整体结构形状，反映同一网络中各实体之间的结构关系。

网络的节点有两类：一类是转换和交换信息的转接节点，包括节点交换机、集线器和终端控制器等；另一类是访问节点，包括计算机主机和终端等，它们是信息交换的源节点和目标节点。

1.3.2 几种典型的网络拓扑结构

网络的拓扑类型较多，基本的拓扑类型有以下五种：总线型、星型、环型、树型和网状型，如图 1-6 所示为网络的五种基本拓扑类型。

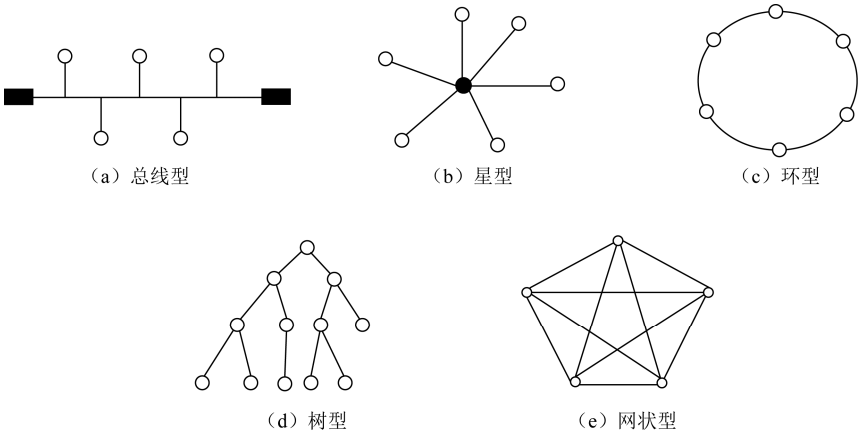


图 1-6　五种基本拓扑类型

1．总线型

总线型结构网络是将各个节点和一根总线相连，总线两端需要连接终结器匹配线路阻抗，防止信号反射回总线产生干扰，如图 1-7 所示。网络中所有的节点都通过总线进行信息传输，任意时候只能有一个节点发送数据，否则将会产生冲突，任何一个节点

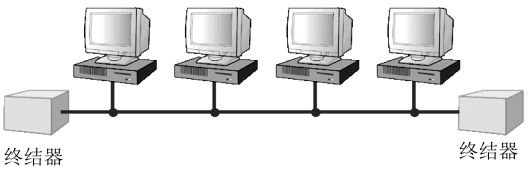


图1-7　总线型拓扑结构

的信息都可以沿着总线向两个方向传输，并被总线中任何一个节点所接收。

（1）总线型网络的主要优点：结构简单灵活，对节点设备的安装、拆卸方便，可扩充性好；总线拓扑所需的电缆数量少，相比其他布线方式便宜；网络节点响应速度快，共享资源能力强，设备投入量少，安装使用方便。

（2）总线型网络的主要缺点：对通信线路（总线）的故障敏感，任何通信线路的故障都会使得整个网络不能正常运行，而且故障的隔离及诊断困难；由于共用一个总线，站点间为了协调通信，需要复杂的介质访问控制机制。如果网络内连接的计算机数量较多，网络效率和传输性能不高。

2．星型

星型结构的网络是以中央节点为中心，用单独的线路将中央节点与各个节点连接起来，各节点之间的通信首先必须要通过中央节点，中央节点接收信息后再转发给相应节点，如图 1-8 所示。中央节点目前多采用集线器或交换机。

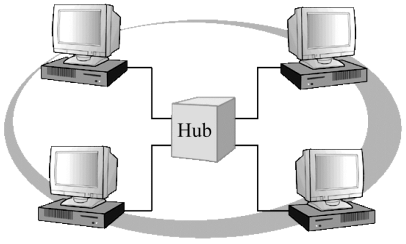


图1-8　星型拓扑结构

（1）星型网络的主要优点：网络结构简单，便于控制和管理、易扩展；单个连接点的故障只影响一个设备、不会影响全网；每个节点直接连到中央节点，故障容易检测和隔离。

（2）星型网络的主要缺点：由于每个节点与中央节点都需一条线缆连接，线缆使用量大，布线施工成本高，同时通信线路的利用率不高；中央节点负担重，容易成为网络的瓶颈，一旦出现故障会造成整个网络的瘫痪，对中央节点的可靠性和冗余度要求高。

3．环型

环型结构中的各节点是连接在一条首尾相连的闭合环型线路中的，如图 1-9 所示。环型网络中的信息传送是单向的，即沿一个方向从一个节点传到另一个节点，当信息流中的目标地址与环上的某个节点的地址相同时，信息被该节点接收，之后信息继续流向下一节点，一直流回到发送该信息的节点为止。

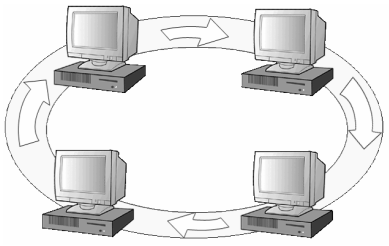


图1-9　环型拓扑结构

（1）环型网络的主要优点：信息流在网络中是沿着固定方向流动的，而且两个节点之间仅有一条路径，结构简单，由此使得路径选择、通信接口、软件管理都比较简单，所以实现起来比较容易。

（2）环型网络的主要缺点：任何节点的故障均能导致环路不能正常工作，造成整个网络的中断与瘫痪，因此可靠性较差，同时，与总线型网络相似，维护困难，目前已有许多方法如建立双环结构等，来解决此问题；另外当节点过多时，会影响传输效率，使网络响应时间变长；在加入新的工作站时必须使环路暂时中断，故不利于系统扩充。

4．树型

树型结构是总线型结构的扩展，它是在总线网上加上分支形成的，其传输介质可有多条分支，但不形成闭合回路，也可以把它看成是星型结构的叠加，如图 1-10 所示。树型是分级的集中控制式网络，节点按层次进行连接，最上面的主节点通过各级中心节点对网络进行分级管理，信息交换主要在上下节点之间进行。树型结构虽有多个中心节点，但各个中心节点之间很少有信息流通。

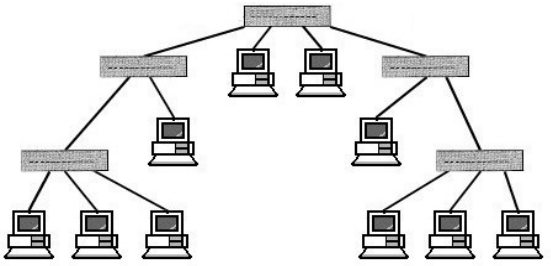


图1-10　树型拓扑结构

（1）树型网络的主要优点：通信线路连接简单，易于扩展，在树型结构中增加新节点和新分支很容易；维护方便，故障易隔离，如果某一分支的节点或线路发生故障，很容易将故障分支或线路与整个系统隔离开来。

（2）树型网络的主要缺点：对根的依赖性太大，如果根发生故障，则全网不能正常工作。

5．网状型

这种拓扑结构是指网络中各节点与通信线路连接成不规则形状，任意一个节点至少与其他两个节点相连。广域网一般采用网状结构，但不常用于局域网，如图 1-11 所示。

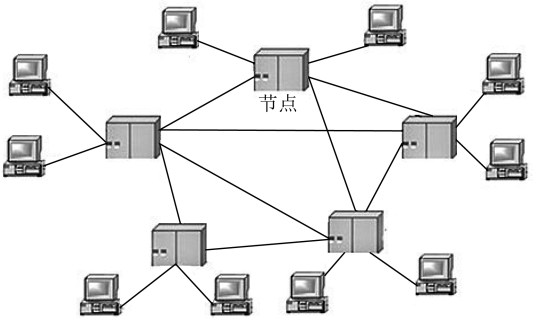


图1-11　网状型拓扑结构

（1）网状型网络的主要优点：由于节点间存在多条传输路径，传输效率高，冗余性能好；另外当某一线路或节点出现故障时，也不会影响整个网络的正常工作，具有较高的可靠性。

（2）网状型网络的主要缺点：网络结构复杂，在多条传输路径中，必须采用合适的路由算法，选择最佳路径传输；布线难度大，建设成本高，不易管理和维护。

1.4　计算机网络的标准及标准化组织

1．国际标准化组织（ISO）

ISO 成立于 1946 年，是一个全球性的非政府组织，也是目前世界上最大、最有权威性的国际标准化专门机构。ISO 与 600 多个国际组织保持着协作关系，其主要活动是制定国际

标准，协调世界范围的标准化工作，组织各成员国和技术委员会进行情报交流，以及与其他国际组织进行合作，共同研究有关标准化问题。

截至 2002 年 12 月底，ISO 已制定了 13736 个国际标准。例如，著名的具有七层协议结构的开放系统互联参考模型（OSI）、ISO9000 系列质量管理和品质保证标准等。

2．美国国家标准协会

ANSI（American National Standards Institute）是成立于 1918 年的非营利性质的民间组织，同时也是一些国际标准化组织的主要成员，如国际标准化委员会和国际电工委员会（IEC）。ANSI 标准广泛应用于各个领域，典型应用有美国标准信息交换码（ASCII）和光纤分布式数据接口（FDDI）等。

3．电气与电子工程师协会（IEEE）

IEEE（Institute of Electrical and Electronics Engineers）成立于 1963 年，由从事电气工程、电子和计算机等有关领域的专业人员组成，是世界上最大的专业技术团体。IEEE 是一个跨国的学术组织，目前拥有 36 万会员，近 300 个地区分会分布在 150 多个国家。IEEE 下设许多专业委员会，其定义或开发的标准在工业界有极大的影响和作用力。例如，1980 年成立的 IEEE802 委员会负责有关局域网标准的制定事宜，制定了著名的 IEEE802 系列标准，如 IEEE802.3 以太网标准、IEEE802.4 令牌总线网标准和 IEEE802.5 令牌环网标准等。

4．国际电信联盟（ITU）

1865 年 5 月，法、德、俄等 20 个国家为顺利实现国际电报通信，在巴黎成立了一个国际组织“国际电报联盟”；1932 年，70 个国家的代表在西班牙马德里召开会议，“国际电报联盟”改为“国际电信联盟”；1947 年，国际电信联盟成为联合国的一个专门机构。国际电信联盟是电信界最有影响的组织，也是联合国机构中历史最长的一个国际组织，简称“国际电联”或 ITU。联合国的任何一个主权国家都可以成为 ITU 的成员。

ITU（International Telecommunication Union）是世界各国政府的电信主管部门之间协调电信事务的一个国际组织，它研究制定有关电信业务的规章制度，通过决议提出推荐标准，收集相关信息和情报，其目的和任务是实现国际电信的标准化。

ITU-T 制定的标准被称为“建议书”，是非强制性的、自愿的协议。由于 ITU-T 标准可保证各国电信网的互联和运转，所以越来越广泛地被世界各国所采用。

5．国际电工委员会（IEC）

IEC（International Electrotechnical Commission）成立于 1906 年，至今已有一百多年的历史，它是世界上成立最早的国际性电工标准化机构，负责有关电气工程和电子工程领域中的国际标准化工作。ISO 正式成立后，IEC 曾作为电工部门并入，但是在技术和财务上仍保持独立性。1979 年 ISO 与 IEC 达成协议：两者在法律上都是独立的组织，IEC 负责有关电气工程和电子工程领域中的国际标准化工作，ISO 则负责其他领域内的国际标准化工作。

6．电子工业协会（EIA）

EIA（Electronic Industries Association）是美国的一个电子工业制造商组织，成立于 1924 年。EIA 颁布了许多与电信和计算机通信有关的标准。例如，众所周知的 RS-232 标准，定义了数据终端设备和数据通信设备之间的串行连接。这个标准在今天的数据通信设备中被广泛采用。在结构化网络布线领域，EIA 与美国电信行业协会（TIA）联合制定了商用建筑电信布线标准（如 EIA/TIA568 标准），提供了统一的布线标准并支持多厂商产品和环境。

习　题　1

一、填空题

1．1969 年，美国国防部高级研究计划局建成了_____实验网，从而形成了早期的计算机网络。

2．1980 年 2 月，在旧金山成立的国际电子电气工程师协会（IEEE）也在 OSI/RM 标准的基础上制定了_____局域网标准。

3．1984 年国际标准化组织（ISO）正式颁布了一个开放系统互联参考模型的国际标准_____。

4．1993 年底国家有关部门决定兴建“_____”、“_____”、“_____”工程，简称“三金”工程。

5．目前，计算机网络正朝着高速化、_____、_____、集成化和_____的方向不断深入发展。

6．从 1987 年 9 月 20 日北京计算机技术研究所的_____教授发出第一封_____开始，标志着 Internet 已经成为中国人生活的一部分，拉开了 Internet 在我国发展的序幕。

7．计算机网络的主要功能是_____、_____、_____、_____和_____。

8．按网络拓扑结构分类，计算机网络一般分为_____、_____、_____、_____和_____等五种。

9．计算机网络由_____子网和_____子网组成，_____子网的主要功能是提供网络通信功能；_____子网是网络中实现资源共享的设备和软件的集合，主要负责全网的信息处理，为网络用户提供各种网络资源及网络服务。

10．“资源共享”中的“资源”是指计算机网络中所有的_____、_____和_____资源。

11．根据网络的覆盖范围和计算机之间互联的距离划分，可以将网络划分为_____、_____和_____三种类型。

12．按网络传输介质的不同将网络分为_____和_____。

13．按照网络使用的传输技术可以分为_____和_____两种类型。

14．网络的“_____”是指网络中节点与线路之间的几何连接形状。

15．ISO 成立于 1946 年，是一个全球性的非政府组织，也是目前世界上最大、最有权威性的_____专门机构。

二、选择题

1．计算机网络是计算机技术和（　　）紧密结合的产物。

A．人工智能　　B．通信技术

C．集成电路　　D．无线技术

2．计算机网络的最大优点是（　　）。

A．速度快　　B．精度高

C．共享资源　　D．安全可靠

3．下面不属于计算机网络功能的是（　　）。

A．资源共享　　B．分布处理

C．数据通信　　D．数据分析

4．按照计算机网络的（　　），可以划分为总线型、环型和星型等类型。

A．通信能力　　B．拓扑结构

C．地域范围　　D．使用功能

5．在星型网络中，常见的中央节点是（　　）。

A．路由器　　B．交换机

C．网络适配器　　D．调制解调器

6．下列网络拓扑结构中，需要使用终结器的拓扑结构是（　　）。

A．总线型　　B．星型

C．网状结构　　D．环型

7．只允许数据在传输介质中单向流动的拓扑结构是（　　）。

A．总线型　　B．星型

C．网状结构　　D．环型

8．一旦中心节点出现故障，则整个网络将会瘫痪的网络拓扑结构是（　　）。

A．总线型　　B．星型

C．网状结构　　D．环型

9．在计算机网络术语中，WAN 的含义是（　　）。

A．以太网　　B．广域网

C．互联网　　D．局域网

10．在计算机网络术语中，LAN 的含义是（　　）。

A．以太网　　B．广域网

C．互联网　　D．局域网

11．一座大楼内的计算机网络系统，属于（　　）。

A．WAN　　B．LAN

C．PAN　　D．MAN

12．客户机/服务器网络，常称为（　　）网络，

A．模拟　　B．C/S

C．B/S　　D．数字

13．广域网与局域网之间的主要区别在于（　　）。

A．采用的传输协议不同　　B．网络覆盖范围不同

C．网络用户不同　　D．通信介质不同

14．小型办公网络中最常用的网络传输介质为（　　）。

A．红外线　　B．同轴电缆

C．双绞线　　D．光纤

15．下列拓扑结构中，可靠性最高的是（　　）。

A．星型　　B．总线型

C．环型　　D．网状型

三、简答题

1．什么是计算机网络？

2．ARPANET 实验网的特点是什么？

3．计算机网络的发展经历了哪几个阶段？

4．组成一个基本的计算机网络需要哪些条件？

5．简述计算机网络的主要功能。

6．计算机网络的主要拓扑结构有哪些？各有什么优缺点？

7．计算机网络的发展趋势是什么？

8．计算机网络是如何分类的？

9．有线网络与无线网络各有何优点？

10．知名的计算机网络标准化组织有哪些？

第2章 数据通信基础

内容摘要

- 数据通信的基础概念
- 数据通信系统的模型
- 数据传输介质
- 数据传输技术
- 多路复用技术
- 数据交换技术
- 差错控制技术

学习目标

- 掌握数据通信的基础概念
- 理解数据通信系统的模型
- 熟悉数据传输介质的特性
- 掌握各种数据传输技术的特点
- 理解多路复用技术原理与应用
- 理解数据交换技术的概念与方法
- 了解差错控制的编码与控制方法

数据通信是计算机技术与现代通信技术相结合而产生的一种新的通信方式和通信业务。数据通信是计算机网络的基础，也是计算机网络的主要功能之一。数据通信是依照通信协议，利用数据传输技术在两个功能单元之间传递数据信息。

数据通信技术的基本作用是完成两个实体间数据的交换，实现计算机与计算机、计算机与终端以及终端与终端间的数据信息的传递。

2.1　数据通信概述

数据通信与传统的语音通信、无线电广播通信不同。它是通信技术和计算机技术相结合而产生的一种新的通信方式，它有着区别于其他通信方式的规律和特点。

2.1.1　基本概念

1．信息、数据

通信的目的是传输、交换信息。数据是传送信息的载体，是信息的数字化形式，所表示的内容就是信息，信息则是对数据的解释，即对数据蕴含内容的说明。信息的表现形式可以是数值、文字、图形、声音、图像、视频以及动画等媒体，这些媒体形式归根到底都是数据的一种形式。

通信双方产生的数据可分为模拟数据和数字数据。模拟数据是指在一定时间间隔内连续变化的值，因具有连续性，所以它可以取无限多个值，例如声音、电视图像信号、温度变化等都是连续变化的，都属于模拟数据，如图 2-1（a）所示；数字数据，是表现为离散量的数据，只能取有限个数值，例如在计算机中用二进制代码表示的字符、图形、音频与视频数据，如图 2-1（b）所示。

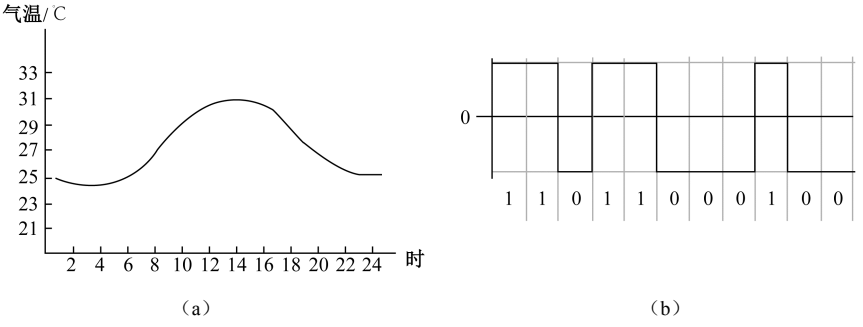


图2-1　模拟数据和数字数据

2．模拟信号和数字信号

信号是数据在传输过程中电信号的表示形式，或称数据的电编码或电磁编码。在数据通信系统中，数据需要转换为信号才可以从一个点传到另一个点。根据电信号的不同形式，信号可分为模拟信号和数字信号。

模拟信号是在一定范围内可以连续取值的信号，是一种连续变化的电信号（如语言信号），它可以以不同频率在介质上传输，如图 2-2（a）所示。数字信号是一种离散的脉冲序列，它的取值是有限个数的，它以恒定的正电压/负电压或正电压/零电压，表示“1”、“0”，可以以不同的位速率在介质上传输，如图 2-2（b）所示。

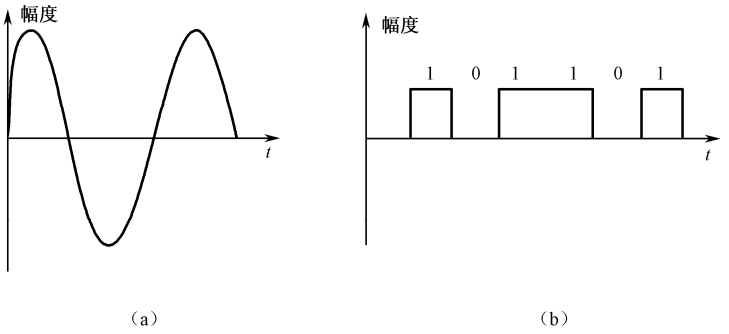


图 2-2　模拟信号和数字信号

在数据通信系统中，信息、数据和信号相互依存又相互独立，通过下面的事例，我们可以深入了解这三者之间的关系。

例如，某同学各科平均考试成绩 99 分，这是一个数据，它蕴含着该同学成绩优秀的信息，如果用高电平表示“1”，低电平表示“0”，则该数据的电编码表示如图 2-3 所示。成绩数据在二进制下表示为 1100011，尽管其形式与 99（十进制）不同，但它表示该同学“成绩优秀”的信息没有变化。

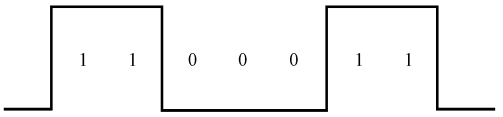


图2-3　信号的电编码

从上面的表述中可以得出如下结论：数据是信息的载体，信息是数据的内容和解释，而信号是数据的编码。

3．信道

要在两个实体间传输信息必须通过传输信道将数据终端与计算机连接起来，从而使不同地点的数据终端实现软、硬件和数据资源的共享。

信道是指两地间传输数据信号的通路，即信号的传输通道，包括通信设备和传输介质。不同的信道用来传递不同的信号，信道不同，信道的物理特性不同，通信的速率和通信的质量也不同。

信道可以按不同的方法分类：按传输介质分为有线信道（介质包括电缆、光缆等）和无线信道（如传输电磁波的空间）；按照使用权限分为专用信道和公用信道；按传输信号的形式可以分为模拟信道和数字信道，模拟信道用于传输模拟信号，数字信道用于传输数字信号。

2.1.2　数据通信系统

1．数据通信系统的模型

数据通信系统的基本组成一般包括发送端、接收端以及收发两端之间的信道三个部分，

如图 2-4 所示。

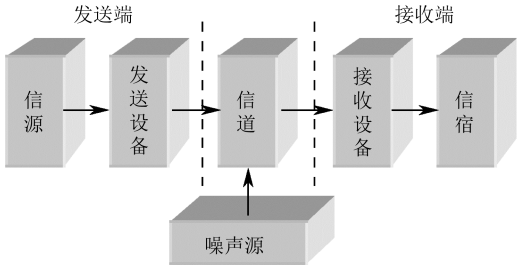


图 2-4　数据通信系统的模型

信源是信息或信息序列的产生源，它泛指一切发信者，可以是人也可以是机器设备，能够产生诸如声音、数据、文字、图像、代码等电信号。信源发出信息的形式可以是连续的，也可以是离散的。

发送设备把信源发出的信息变换成便于传输的形式，使之适应于信道传输特性的要求并送入信道的各种设备。发送设备是一个整体概念，可能包括许多的电路、器件与系统。例如，把声音转换为电信号的麦克风，把基带信号转换成频带信号的调制器等。

信道是指传输信号的通道，包括通信设备和传输介质。

接收设备接收从信道传输过来的信息，并转换成信宿便于接收的形式，其功能与发送设备的功能刚好相反。接收设备也是一个整体概念，可能包括许多的电路、器件与系统，如将模拟信号转换为数字信号的解调器等。

信宿是接收发送端信息的对象，它可以是人，也可以是机器设备。

信号在信道中传输可能会受到其他信号的干扰，这种干扰称之为噪声。噪声会影响正常信号的传输，对通信系统而言，它是有害的。噪声既可以来自内部，也可以来自外界，产生干扰的设备叫做噪声源。

2．模拟通信和数字通信

通信系统的基本作用是在发送方（信源）和接收方（信宿）之间传递和交换信息。根据通信系统是利用模拟信号还是数字信号来传递消息，通信系统可分为模拟通信系统和数字通信系统。

模拟通信系统利用模拟信号来传递信息，如普通的电话、广播和电视。模拟通信系统通常由信源、调制器、信道、解调器、信宿及噪声源组成。信源所产生的原始模拟信号一般都经过调制器后再通过信道传输，解调器则将信道上的信号实施逆变换后送达信宿。人们日常使用的拨号上网就是一个模拟通信系统的实例，发送端工作站发送的数据经调制解调器转换为模拟信号后，送到公共电话网上传输，到接收端经调制解调器变换为数字信号后，与服务器通信。模拟通信系统的模型如图 2-5 所示。

数字通信系统利用数字信号来传递信息，如计算机通信、数字电话、数字电视等。数字通信系统由信源、信源编码器、信道编码器、调制器、信道、解调器、信道译码器、信源译码器，以及发送端和接收端 10 部分组成。在数字通信系统中，如果信源发出的信号是模拟信号，则要经过信源编码器转换为数字信号；信道编码器对信号进行检错纠错编码以

实现差错控制；译码器则实现编码器的逆变换；调制器将编码器输出的基带信号调制成频带信号在信道上传输；解调器的功能正好相反。数字通信系统的模型如图 2-6 所示。

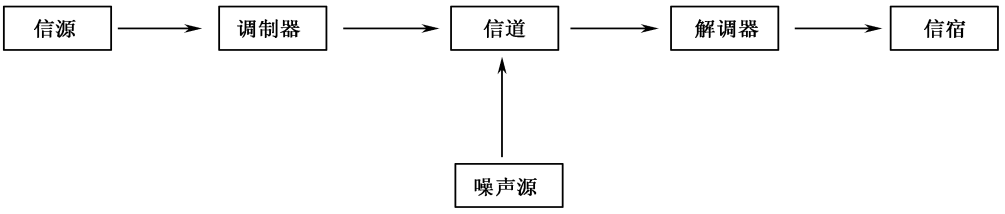


图 2-5　模拟通信系统的模型

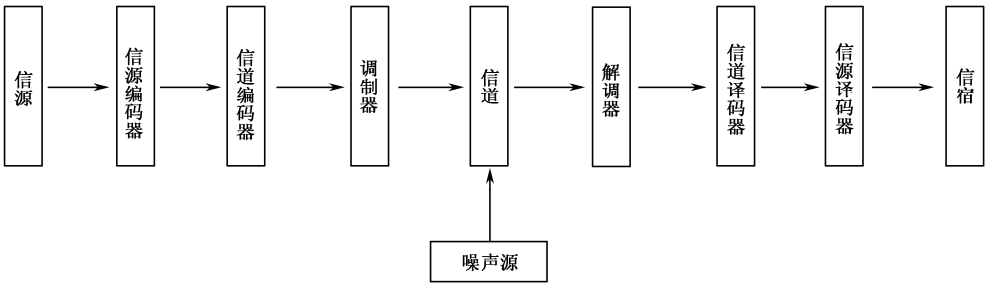


图 2-6　数字通信系统的模型

两种通信系统在远程传输时都会面临信号衰减的问题。模拟传输系统为了实现长距离传输，要用放大器来增强信号中的能量，但同时也会使噪声增强，以至于引起信号畸变。数字传输系统的衰减也会影响数据的完整性，数字信号只能在一个有限距离内传输，为了获得更大的传输距离，可以使用中继器。中继器接收衰减了的数字信号，把数字信号恢复为“0”、“1”的标准水平，然后重新传输这种新的信号，这样就有效地克服了衰减。

模拟通信在通信系统中曾经占据着主导地位，但是随着大规模集成电路技术、计算机技术，以及数字信号处理技术的发展，大多数的模拟通信系统被数字通信系统所取代。究其原因，模拟通信存在保密性差，抗干扰能力弱等缺点。而数字通信有着抗干扰能力强，可以实现信号的差错控制，易加密和解密，传输可靠性高等诸多优点。尽管数字通信也存在着频带利用率低，技术要求复杂等缺点，但是由于数字通信的性能远远超越了模拟通信，所以在现在的通信系统中，数字通信系统已经逐步取代了模拟通信系统，成为数据通信的主要发展方向。

参考链接

在通信系统中，设备与设备之间通信线路的连接方式有两种，分为多点连接和点到点连接。多点连接指网络上的所有机器共享一条通信信道，一台机器发送数据包，可以被网络上所有其他机器接收，但是只有目标地址相符的机器才会处理该数据包，其他的则将数据包丢弃；点到点连接指计算机之间直接用线路或通过调制解调器用线路连接，使用的线路既可以是专用线路，也可以是租用的线路。一般来说，地理位置上处于本地的网络采用多点连接，而大的网络则采用点到点的连接。

2.1.3 数据的编码与调制

在数据通信系统中，数字信道一般只用来传输数字信号，模拟信道一般只用来传输模拟信号。但是有时也可能需要用数字信道来传输模拟信号，或用模拟信道来传输数字信号。但是数字信号不可能通过为模拟信号设计的传输线路（如电话传输线）传送，反之亦然。这时，我们必须先对要传输的数据进行转换，转换为信道可以传送的信号，这就需要编码或调制，使之与传输介质相适应，这样才能够正确无误地传送到目的端。

用数字信号承载数字或模拟数据，称为编码。用模拟信号承载数字或模拟数据，称为调制。

一般来说，有四种传输数据的方法。

数字数据的数字信号编码：把数字数据转换成某种数字脉冲信号，常见的有两类，不归零码和曼彻斯特编码。

模拟数据的数字信号编码：一般通过脉冲编码调制方法将模拟数据量化为数字信号，这常用于对声音信号编码。

数字数据的模拟信号调制：三种常用的调制技术是幅移键控法、频移键控法、相移键控法。

模拟数据的模拟信号调制：最常用的两种调制技术是幅度调制和频率调制。

2.1.4 数据通信的常用术语

码元：码元是对于网络中传送的二进制数字中每一位的通称，也常称为“位”或 bit。例如字母 A 的 ASCII 码是 1000001，可认为由 7 个码元组成，共有 7 位。

噪声源：一个通信系统不可避免地存在噪声干扰，为了研究问题方便，把它们等效于一个作用于信道上的噪声源。

信道容量：信道容量指信道能传输信息的最大能力，一般以单位时间内最大可传送信息的位数表示。在使用中，信道容量应大于传输速率，否则高的传输速率得不到充分发挥利用。

响应时间：从发送一条信息到收到回答之间的时间。例如，有关更新名字一地址文件中一个记录的请求就是一条信息，而在终端显示屏上显示更新后的一条记录则是一个回答。根据查询的复杂性、分享处理机的终端数目、主计算机的速度以及通道速度的不同，响应时间有很大的差别。

数据传输速率：数据传输速率指通信线上传输信息的速度。有两种表示方法，即信号速率和调制速率。信号速率 S 是指单位时间内所传送的二进制代码的有效位数，以每秒多少比特数来计算，即 bps。调制速率 B 是脉冲信号经过调制后的传输速率，以波特（baud）为单位，通常用于表示调制器之间传输信号的速率。

差错校正：字符代码在传输、接收过程中，难免发生错误，如何及时自动检测差错并进一步自动校正，也是数字通信系统研究的重要课题，通常的解决办法采用抗干扰编码或纠错编码，目前常采用的有奇偶校验码、循环冗余码等。

2.1.5 数据通信中的主要技术指标

在数字通信中，一般使用比特率和误码率来分别描述数据信号传输速率的大小和传输质量的好坏等；在模拟通信中，常使用带宽和波特率来描述通信信道传输能力和数据信号对载波的调制速率。

1．带宽

在模拟信道中，常用带宽表示信道传输信息的能力，带宽即传输信号的最高频率与最低频率之差。例如：一条传输线路可以传输的信号频率范围为 600～1800Hz，那么该传输线路的带宽为 1200Hz。理论分析表明，模拟信道的带宽或信噪比越大，信道的极限传输速率也越高。这也是为什么总是努力提高通信信道带宽的原因。

2．比特率

在数字信道中，比特率是数字信号的传输速率，它用单位时间内传输的二进制代码的有效位（bit）数来表示，其单位为每秒比特数 b/s（bps）、每秒千比特数（kbps）或每秒兆比特数（Mbps）来表示（此处 k 和 M 分别为 1000 和 1000000，而不是涉及计算机存储器容量时的 1024 和 1048576）。

3．波特率

波特率指数据信号对载波的调制速率，它用单位时间内载波调制状态改变次数来表示，其单位为波特（baud）。波特率与比特率的关系为：比特率=波特率×单个调制状态对应的二进制位数。

4．误码率

误码率指在数据传输中的错误率。在计算机网络中一般要求数字信号误码率低于 10^{-6}。

2.2 数据传输介质

人们在构建网络时，都会充分考虑网络的构建成本。网络工程中最大的工程量就是网络布线。在网络布线工程中，需要使用大量的数据传输介质，选择了不恰当的数据传输介质会给整个工程带来很大的浪费，并影响工程质量及工程造价，所以数据传输介质的选择是网络工程中非常重要的环节。

2.2.1 传输介质的基本概念

数据传输介质是指传送信息的载体，是通信网络中发送方和接收方之间的物理通路。因此，传输介质也称为传输媒体、传输媒介或传输线路。不同的数据传输介质对网络的传

输速率、传输距离、抗干扰性、成本、可连接的节点数目以及传输的可靠性等方面都有很大的影响，必须根据不同的通信要求，合理地选择传输介质。

1．传输介质的分类

传输介质分为有线介质和无线介质两大类。网络中常用的有线介质是双绞线、同轴电缆和光纤；常用的无线介质是无线电波、微波和红外线等。

2．传输介质的特性

数据传输的质量除了与传送的数据信号及收发两端的设备特性有关外，还直接与通信线路本身的机械和电气特性有关。这些特性主要包括以下几种。

（1）物理特性：指传输介质的特征。

（2）传输特性：传输信号调制技术、信道容量及传输的频带范围。

（3）覆盖地理范围：指在不用中继设备情况下，无失真传输所能达到的最大距离。

（4）抗干扰特性：指防止噪声对传输信息影响的能力。

（5）价格：指线路安装、维护等费用总和。

2.2.2　双绞线（Twisted Pair）

双绞线是最常见的网络传输介质之一，被广泛应用于电话通信网络和数据通信网络，如图 2-7 所示。双绞线的核心是相互绝缘并缠绕在一起的不同颜色的细芯铜导线对，通常由两对或更多对这样缠绕在一起的导线组成，依靠相互缠绕（双绞）作用，来消除或减少外界以及导线之间产生的电磁干扰（EMI）和射频干扰（RFI）。

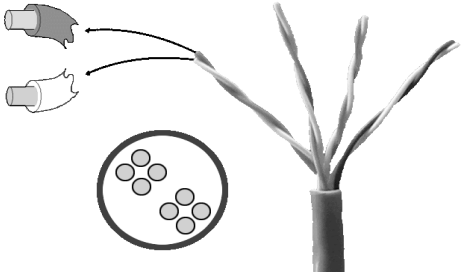


图 2-7　双绞线

双绞线是一种柔性的通信电缆，因此非常适合于墙内、转角等位置布线。双绞线与适合的网络设备相连，可以实现 100Mbps 或者更快速度的网络通信。在大多数应用下，双绞线的最大布线长度为 100m，但是按通常的经验，考虑到网络设备中和配线架要额外布线，所以双绞线的布线长度最好限制在 90m 以内。

根据是否有屏蔽层，双绞线可分为屏蔽双绞线（STP）和非屏蔽双绞线（UTP）。

1．屏蔽双绞线

屏蔽双绞线（Shielded Twisted -Pair，STP）由成对的绝缘实心电缆组成，在实心电缆上

包围着一层用金属丝编织的屏蔽层，如图 2-8 所示。屏蔽层减少了由 RFI 和 EMI 引起的对通信信号的干扰。将一对电线缠绕在一起也有助于减少 RFI 和 EMI，但是在一定程度上不如有屏蔽层的效果好。要更有效地减少 RFI 和 EMI，每一对电线交织的距离必须是不同的。而且，为了获得最好的效果，插头和插座必须要屏蔽。如果线材上某点的主要屏蔽层损伤，信号的畸变就会很严重。

屏蔽双绞线布线时，另一个重要因素是要正确接地，以获得可靠的传输信号控制点。在周围有重型电力设备和强干扰源的位置，推荐使用屏蔽双绞线。屏蔽双绞线、屏蔽型插头连同兼容的网络设备价格相对较高，安装时也要比非屏蔽双绞线困难，所以成本相对更高。

2．非屏蔽双绞线

非屏蔽双绞线（Unshielded Twisted-Pair，UTP），也就是人们平时所用的网线，由于其价格相对低廉且易于安装，是人们在局域网组网布线中使用最多的网络电缆。UTP 由位于绝缘保护层内的成对的电缆线组成，缠绕在一起的绝缘电线和电缆外部的套之间并没有屏蔽，如图 2-9 所示。由于没有屏蔽层，所以非屏蔽双绞线的抗干扰性比屏蔽双绞线差，但是非屏蔽双绞线直径小、重量轻、易弯曲、易安装、成本低，所以网络中大量使用非屏蔽双绞线作为传输介质。

图2-8　屏蔽双绞线

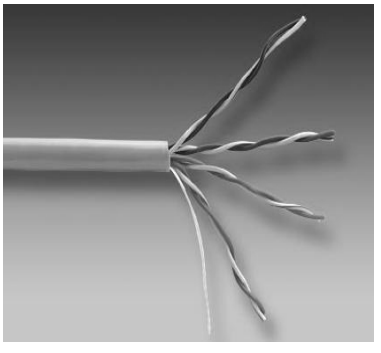


图2-9　非屏蔽双绞线

双绞线的技术标准主要由电子工业协会/电信工业协会（EIA/TIA）制定的。1991 年，电子工业协会/电信工业协会（EIA/TIA）联合发布了一个标准 EIA/TIA-568，它的名称是“商用建筑物电信布线标准”，该标准规定了非屏蔽双绞线工业标准。随着局域网数据传输速率的不断提高，布线标准也在不断更新，目前应用最广的是 EIA/TIA-568B 标准。

非屏蔽双绞线（UTP）按照电气性能划分，通常可分为：1 类、2 类、3 类、4 类、5 类、超 5 类、6 类等类型，各类型的特点如表 2-1 所示。

表 2-1　常用非屏蔽双绞线

类　　型	最高传输频率	最高传输速率	主 要 应 用
1 类线	750kHz	20kbps	主要用于传输语音
2 类线	1MHz	4Mbps	语音传输和 4Mbps 的令牌网
3 类线	16MHz	10Mbps	语音传输和 10Mbps 的以太网

续表

类　　型	最高传输频率	最高传输速率	主 要 应 用
4 类线	20MHz	16Mbps	语音传输、令牌网和 100Mbps 的以太网
5 类线	100MHz	100Mbps	语音传输和 100 BASE-T 以太网
超 5 类线	200MHz	1000Mbps	语音传输、百兆位的快速以太网及千兆网
6 类线	250MHz	2.4Gbps	语音传输、百兆位的快速以太网及千兆网

3．双绞线的制作

将双绞线两端连接上 RJ-45 接口，就成为一条网络连接电缆。制作网络连接电缆是人们连接网络最基本的工作之一。要制作线缆，首先需要了解一下制作网络连接电缆所需要的材料和工具。

（1）线缆

制作网络连接电缆，首先要准备 UTP 线材，现在广泛使用较多的是超五类的双绞线。现在市场上的普通线材大都采用硬质纸盒包装（工程用线也有无包装的散装线材），外包装上标识着线材的品牌、型号、阻抗、线芯直径等技术参数。通常，一箱线材的长度为 1000 英尺，约合 305m。

参考链接

在线材上，每隔一段距离，会有一段文字标识，描述线材的一些技术参数，不同生产商的产品标识可能略有不同，但一般应包括以下一些信息：双绞线的生产商和产品编码、双绞线类型、NEC/UL 防火测试和级别、CSA 防火测试、长度标志和生产日期等。以下用一个实例来介绍双绞线上的标识：

“AMP NETCONNECT CATEGORY 5e CABLE E13804 1300 24AWG CM（UL）CMG/MPG（UL）VERIFIED TO CAT 5 000088022FT 0927”。

其中：AMP NETCONNECT 为线缆生产厂商标识，此例生产商为安普公司；

CATEGORY 5e CABLE 表示该双绞线属于 CAT E5 类，即超五类线材；

E13804 1300 为电缆产品型号；

24 AWG 说明双绞线是由 24 AWG 直径的线芯构成的，铜电缆的直径通常用 AWG（American Wire Gauge）单位来衡量，通常 AWG 数值越小，电线直径越大，常见的有 22/24/26 等；

CM（UL）CMG/MPG（UL）说明线材属于通信通用电缆，CM 是 NEC（美国国家电气规程）中防火耐烟等级中的一种，UL 说明双绞线满足 UL（Underwriters Laboratories Inc.，保险业者实验室）的标准要求，UL 成立于 1984 年，是一家非营利性的独立组织，致力于产品的安全性测试和认证；

VERIFIED TO CAT 5 表示通过五类线的测试标准；

000088022FT 表示当前位置，以英尺为单位，1 英尺等于 0.3048m；

0927 为生产日期，其中前两位为年份，后两位为星期，本例表示该线缆的生产日期 2009 年第 27 周。

（2）RJ-45 接口

RJ 这个名称代表已注册的插孔（Registered Jack），是来源于贝尔系统的 USOC（Universal Service Ordering Codes，通用服务分类代码）代码，USOC 是一系列已注册的插孔及其接线方式，由著名的贝尔公司开发，用于将用户的设备连接到公共网络。

RJ-45 是当前在局域网连接中使用最常见的网络接口，如图 2-10 所示。以与线材接压简单，连接可靠著称。常见的应用场合有以太网接口、ATM 接口及一些网络设备（如 Cisco）的控制（Console）口等。

RJ-45 接口采用透明塑料材料制作，由于其外观晶莹透亮，常被称为“水晶头”。RJ-45 接口具有 8 个铜制引脚，在没有完成压制前，引脚凸出于接口，引脚的下方是悬空的，有两到三个尖锐的突起，如图 2-11 所示。在压制线材时，引脚向下移动，尖锐部分直接穿透双绞线铜芯外的绝缘塑料层与线芯接触，很方便地实现接口与线材的连通。有个需要特别注意的问题是，由于没有压制的 RJ-45 接口，引脚与插座接触部分还处于凸出的状态，因此严禁将没有制作的 RJ-45 接口插入 RJ-45 插座中，否则会造成接口损坏。

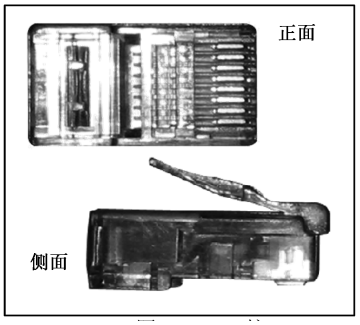


图 2-10　RJ-45 接口

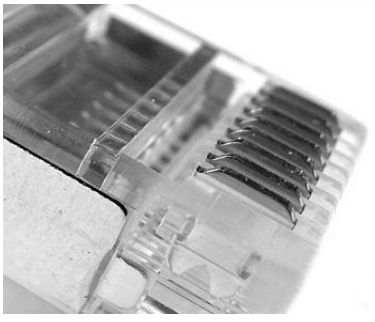


图 2-11　RJ-45 接口引脚

（3）压线钳

为了制作网络连接电缆，还要准备几种工具，压线钳是其中之一，如图 2-12 所示。压线钳规格型号很多，分别适用于不同类型接口与电缆的连接，通常用 XPYC 的方式来表示（其中 X、Y 为数字），P 表示接口的槽位（Position）数量，常见的有 8P、4P 和 6P，分别表示接口有 8 个、4 个和 6 个引脚凹槽；C 表示接口引脚连接铜片（Contact）的数量。如人们常用的标准网线接口为 8P8C，表示有 8 个凹槽和 8 个引脚。常用的电话通信电缆接口为 4P2C，表示有 4 个凹槽和 2 个引脚。在制作电缆前要根据实际情况选择合适的压线钳。

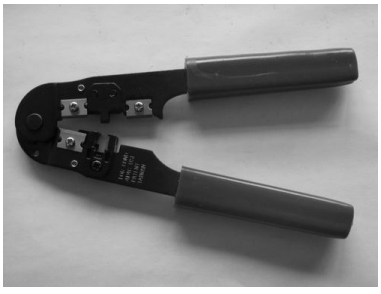


图 2-12　压线钳

即使确定了选用的电缆、接口和工具，制作的电缆仍有多种不同的类型，分别适用于不同的场合。网络连接电缆可以分为三类：直通缆、交叉缆和全反缆，分别适用于不同设备接口之间的连接。直通缆顾名思义，两端的线序是一致的；交叉缆两端线序不同，一端的引脚 1 与引脚 2 分别连接到对端的引脚 3 和引脚 6；而全反线两端的线序正好完全相反。EIA/TIA-568A 和 EIA/TIA-568B 标准接口线序如表 2-2 所示，不同类型的网络电缆适用场合如表 2-3 所示。

表 2-2　EIA/TIA-568A 与 EIA/TIA-568B 接口线序

类　　型	1	2	3	4	5	6	7	8
T568A	白绿	绿	白橙	蓝	白蓝	橙	白棕	棕
T568B	白橙	橙	白绿	蓝	白蓝	绿	白棕	棕

表 2-3　不同网络电缆的适用场合

电 缆 类 别	标准接口线序	适 用 场 合
直通缆	EIA/TIA-568A－EIA/TIA-568B EIA/TIA-568A－EIA/TIA-568B	计算机—集线器、计算机—交换机、 路由器—集线器、路由器—交换机、 集线器/交换机（Uplink 级联口）—集线器/交换机
交叉缆	EIA/TIA-568A－EIA/TIA-568B	计算机—计算机、路由器—路由器、 集线器—集线器、交换机—交换机、 集线器—交换机
全反缆	—	Cisco 等网络设备 Console（控制口）专用

为了记忆简单，可以认为计算机与路由器是一类设备，集线器与交换机是一类设备，同类设备相连使用交叉缆，不同设备之间相连使用直通缆，而级联口则是为了连接设备方便，在接口电路内部已经进行了转换。因此，级联口与普通接口相连，即使是同类设备也使用直通缆。

（4）双绞线的制作过程

下面来了解一下网络电缆的制作过程。

① 利用压线钳的剪线刀口剪下所需长度的双绞线，接着利用压线钳的剥线刀口将双绞线的外护套除去 2.5cm 左右。

② 小心地拆开每一对线芯，按照规定的线序将拆开的线芯排列起来，要注意排列好的线芯尽可能地不发生缠绕，否则在将线芯插入 RJ-45 接口时容易发生线芯移位而造成线序错误。

③ 将排好线序的线芯拉直，排列整齐，并仔细检查线序是否保持正确。

④ 将整理好的线芯用压线钳剪线口修剪剩约 14mm 的长度，之所以留下这个长度是为了符合 EIA/TIA 的标准，能保证在线芯插入正确位置后，外层护套能被 RJ-45 后端的护套卡口固定住，保证在插拔线材时纤细的内芯不会因受力而损坏。

⑤ 将线芯插入 RJ-45 接口，注意此时 RJ-45 接口正面朝上（即接口铜制引脚露出部分应朝上方和外侧），并确定每一根线芯都插入接口最顶端。

⑥ 确定双绞线的每根线芯都已正确放置之后，就可以用压线钳压接。市场上还有一种接头的保护套，可以防止接头在拉扯时造成接触不良，使用这种保护套时，需要在压接接头之前就将这种胶套插在双绞线电缆上。

⑦ 重复以上步骤，制作另一端的 RJ-45 接头，要注意选择的线型对应的线序。

图 2-13　简易网线测试仪

完成线缆制作后，可以采用简易网线测试仪对电缆导通情况和线序情况进行检查，简易网线测试仪分两个部分，一个部分是主机，上面有对应的网络接口插座，另一部分是终结口，可以从主机上分离，也提供对应的网络接口插座，如图 2-13 所示。

进行测试时，将网络电缆的两端分别插入测试仪的两个插座中，打开开关，可以观察两个部分上提供的 LED 指示灯，在测试过程中，这些指示灯应循环依次闪亮，如果中间有部分指示灯不亮，表示对应的线芯不导通；如果发生主机、终结侧 LED 指示灯闪亮编号不一致，则表示线序不正确（当然交叉线应该 1/3、2/6 对换指示）。

2.2.3 同轴电缆

同轴电缆由四层按“同轴”形式构成，如图 2-14 所示。从里向外分别是内芯、绝缘层、屏蔽层和绝缘外套。

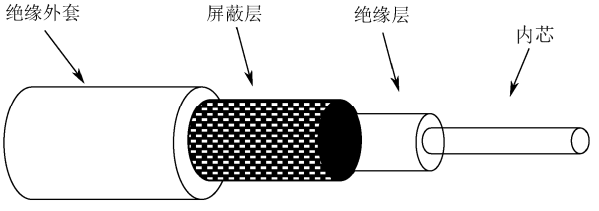


图 2-14　同轴电缆结构

（1）内芯：金属导体，用于传输数据。
（2）绝缘层：用于内芯与屏蔽层间的绝缘。
（3）屏蔽层：金属导体，用于屏蔽外部的干扰。
（4）绝缘外套：用于保护电缆。

1．同轴电缆的物理特性

同轴电缆内芯一般是铜质的，能提供良好的传导率。同轴电缆分为基带同轴电缆和宽带同轴电缆两类。

（1）基带同轴电缆

采用基带传输，即采用数字信号进行传输，用于构建 LAN。常用的基带同轴电缆有两种：50Ω，RG-8 和 RG-11（用于粗缆以太网）；50Ω，RG-58（用于细缆以太网）。

（2）宽带同轴电缆（75Ω，RG-59）

采用宽带传输，即采用模拟信号进行传输，用于构建有线电视网。

2．同轴电缆的其他特性

（1）传输特性

基带同轴电缆用于传输数字信号，采用曼彻斯特编码，速率最高可达 10Mbps。

宽带同轴电缆既可以传输模拟信号，又可以传输数字信号。

（2）连通性

可用于点到点连接和多点连接。

（3）地理范围

典型基带同轴电缆的最大距离限制在几千米内，宽带同轴电缆可达十几千米。但是在 10BASE5 粗缆以太网中，传输距离最大为 500m；在 10BASE2 细缆以太网中，传输距离最大为 185m。

（4）抗干扰性

抗干扰性通常高于双绞线。

（5）价格

高于双绞线，低于光纤。

2.2.4 光纤

光纤通信是一门新兴的通信技术，发展非常迅速，现已成为大容量通信领域中的主要支柱。光纤通信从完成基础研究到大规模应用，只花费了短短的 20 多年的时间，就实现了从短距离、低速光纤通信到长距离、高速光纤通信的飞跃，现已成为现代通信的基石。

1．光缆的结构

光导纤维是一种传输光束的细而柔韧的介质，光导纤维电缆由一捆纤维组成，简称光缆。如图 2-15 所示为室内光缆，如图 2-16 所示为室外光缆。

图 2-15　室内光缆

图 2-16　室外光缆

光缆是数据传输中最有效的一种传输介质，光缆中传输数据的是光纤，光纤是光导纤维的简称，是一种细小、柔韧并能传输光信号的介质。其结构包括纤芯、包层和涂覆层。纤芯由许多细如发丝的玻璃纤维组成，位于光纤的中心部位，是高度透明的材料；

包层的折射率略低于纤芯，从而可以使光电磁波束缚在纤芯内并可长途传输。包层外涂覆一层很薄的环氧树脂或硅橡胶，其作用是保护光纤不受水汽侵蚀，免受机械擦伤，增加柔韧性。

2．光纤的种类

根据光在光纤中的传播方式，光纤可分为两种类型即多模光纤和单模光纤。所谓“模”是指以一定角度进入光纤的一束光。如果光纤导芯的直径小到只有一个光的波长，光纤就成了一种波导管，光线就不必经过多次反射式的传播，而是一直向前传播，这种光纤称为单模光纤。只要到达光纤表面的光线入射角大于临界角，便产生全反射，因此可以由多条入射角度不同的光线同时在一条光纤中传播，这种光纤称为多模光纤。

（1）单模光纤

单模光纤中心纤芯很细（纤芯直径一般为 8～10μm），采用激光二极管做光源，只能允许一束光传播，所以单模光纤没有模分散特性，传输距离可以达到几十千米至上百千米，因而适用于远程通信。单模光纤的传输频带宽，容量大，传输距离长，但因其需要激光源，成本较高，通常在建筑物之间或地域分散时使用。

（2）多模光纤

多模光纤的纤芯较粗（纤芯直径为 50～62.5μm），可传送多种模式的光源。但其模间色散较大，这就限制了传输数字信号的频率，而且随距离的增加，模间色散会更加严重，因此，多模光纤传输的距离比较小，一般只有几千米。多模光纤多采用发光二极管做光源，整体的传输性能较差，但多模光纤允许多束光在光纤中同时传播，因此成本较低，一般用于建筑物内或地理位置相邻的环境下。

光纤相比其他网络传输介质有着不可比拟的优势。由于光纤通信时传送的是光束而不是电气信号，而光束在光纤中的传输损耗要比传统电信号在传输线路中的损耗低得多，因此，传输距离大大增加。光纤传输采用的光信号不受电磁干扰的影响，适用于严重电磁干扰的场合。光信号没有电磁感应，不易被窃听，安全性高。光纤体积小，质量轻，便于铺设，耐高温、耐腐蚀，可以适应恶劣的工作环境。此外，光纤的主要原材料是二氧化硅，是地球的主要构成物质，而传统的通信介质的主要原材料是稀有金属（铜和铝），其资源严重短缺，从原材料成本分析，光纤也具有明显的优势。

但光纤也存在着缺点，光纤由于线芯极细，一旦发生断裂，接合难度极大，即便接合成功，衰减也远远超过正常的线路。此外，光纤虽然原材料成本低廉，但加工工艺要求高，生产成本居高不下，造成市面上光纤价格较高。

当前，光纤在长距离信息传输线路中得到广泛的应用。随着光纤价格的下降，光纤的应用也越来越广泛，如医疗、视听娱乐等场合，也常常能见到光纤的身影，随着光纤生产技术的成熟，光纤的价格会越来越低，终将替代铜线成为主要的有线传输介质。

2.2.5 无线传输介质

无线传输介质，就是采用的物理传输介质不是实体的，而是看不见摸不着的。常见的无线传输介质有红外线、无线电波、微波等。

1．红外线传输技术

红外线（Infrared，IR）技术广泛应用在电视机、空调等家用电器的遥控器中，也可以作为网络通信的介质。它通过使用位于红外频率波谱中的锥形或者线型光束来传输数据信号，通信的双方设备都拥有一个收发器，最好还有同步软件，传输速率一般为 4M～16Mbps。

红外通信是一种廉价的无线传输方案，实现简单，被广泛应用于移动设备之上，如便携计算机、个人数字代理（PDA）、手机设备，大都配置了红外传输接口。红外传输接口是便携设备之间进行临时性数据交换时经常用的接口。

红外通信有其非常明显的弊端，首先红外线是一种视线技术，不能通过不透明的物理层（如墙壁），并且易受外界光线干扰；其次红外通信有效距离很短，一般在几米之内，因此红外技术并不适合作为连接网络的主要方式。

当前，红外技术在计算机系统中更多的应用集中于外围设备，如红外键盘、鼠标等，这是因为相比其他无线技术，红外技术更省能源，采用同样的电池，红外无线鼠标的使用时间长于采用射频技术的无线鼠标。

2．无线电波传输技术

无线电波的频率为 10^4～10^8Hz，含低频、中频、高频、甚高频和特高频，属于管制频段和非管制频段。它很容易产生，传播是全方向的，能从信号源向任意方向进行传播，很容易穿过建筑物，被广泛地应用于现代通信中。由于它的传输是全方位的，所以发射和接收装置不必在物理空间上很准确地对准。

无线电波的特性与频率有关。在较低频率上，无线电波能轻易地通过障碍物，但是能量随着与信号源距离的增大而急剧减小；在高频上，无线电波趋于直线传播并受障碍物的阻挡，还会被雨水吸收。在所有的频率上，无线电波最易受发动机和其他电子设备的干扰，所以它不是一种最佳的传输介质。

无线电通信分为单频通信和扩频通信两种。单频通信指信号的载波频率单一，其载波的可用频率范围遍及整个无线电频率，但单频收发器只能在其中的一个频率下工作。扩频通信使用与其他无线电相同的频率范围，但把信号调制在一个很宽的频率范围上。扩频通信中由于信号能量分布在很宽的频率上，在信号能量不变的前提下，信号强度大大减弱，甚至小于噪声的强度，这样用普通的接收机进行接收时就只能收到噪声而无法分离出信号，当使用扩频接收机时，它将原来展宽的频谱又重新压缩，使得信号强度恢复，从而从噪声中分离出来。

采用无线电波作为网络传输介质的技术很多，如现在最为流行的无线局域网、GPRS、EDGE 等移动通信服务商提供的无线接入网络，在便携设备上广为流行的蓝牙技术等。

3．微波传输

微波系统作为通信手段在我国使用已经有几十年的历史了。在通信卫星使用前，我国的电视网就是依靠大约每 50km 一个微波站来一站一站传送的，这样的微波站属于地面微波系统。在通信卫星使用后，电视信号先传送给同步卫星，再由卫星向地面上转发，覆盖极大的区域，这种系统属于星载微波系统。

微波系统一般工作在较低的兆赫兹频段，地面系统通常为 4G～6GHz 或 21G～23GHz，

星载系统通常为 11G～14GHz，沿着直线传播，可以集中于一点，微波不能很好地穿过建筑物。微波通过抛物状天线将所有的能量集中于一小束，这样可以获得极高的信噪比，发射天线和接收天线必须精确地对准。由于微波是沿着直线传播，所以每隔一段距离就需要建一个中继站。中继站的微波塔越高，传输的距离就越远，中继站之间的距离大致与塔高的平方成正比。

地面微波系统在各个微波站之间用抛物面天线进行通信，在两微波站天线之间应该无任何物体阻隔。由于微波系统中各站之间不需要电缆连接，因此在一些特殊的场合具有不可替代性。例如，需要通过一块荒无人烟的沼泽地，在一个隔江相望的峡谷等处，在这种地方埋设电缆费时费力，有时几乎是不可能，日后的维护也是一项比较困难的事情。在这种情况下，微波站是正确的选择，既节约初始建设费，也方便日后使用和维护。

在星载微波系统中，发射站和接收站设置于地面，卫星上放置转发器。地面站首先向卫星发送微波信号，卫星在接收到该信号后，由转发器将其向地面转发，供地面各站接收。星载系统覆盖面积极大，理论上一颗同步卫星可以覆盖地球 1/3 的面积，三颗同步卫星就可以覆盖全球。用户的地面设备包括一个 0.75～2.4m 直径的抛物面天线、接收机、电缆等。可以将一颗卫星看做一个集线器，各接收站看做一个节点，这样就形成了一个星型网络。

微波通信成本相对比较低，目前已经被广泛地应用于长途电话、蜂窝电话、电视转播等场合。

2.3 数据传输技术

数据在传输信道上的传输方式，按被传输的数据信号的特点，可分为基带传输、频带传输和宽带传输；按传输信道数可分为并行传输与串行传输；按数据传输的方向，可分为单工、半双工和全双工传输。

2.3.1 基带传输

直接使用数字信号传输数据时，数字信号几乎要占用整个频带，终端设备把数字信号转换成脉冲电信号时，这个原始的电信号所固有的频带，称为基本频带，简称基带。在信道中直接传送基带信号时，称为基带传输。基带传输不需要调制、解调，设备花费少，适用于较小范围的数据传输。比如信号从计算机到显示器、打印机等外围设备就是采用基带传输，大多数的局域网也使用基带传输，如以太网、令牌环网。

2.3.2 频带传输

频带传输就是发送端利用调制器将数字信号调制成音频信号（模拟信号），在公共电话线上传输，到达接收端后，再经过解调器的解调，将音频信号还原为原来的数字信号。频带传输不仅克服了目前许多长途电话线路不能直接传输基带信号的缺点，而且能实现多路

复用的目的，从而提高了通信线路的利用率。通常我们所用的调制解调器拨号上网就是利用电话交换网实现计算机之间的数字信号传输，其中调制解调器就是一种能够在数字信号与模拟信号之间进行转换的设备。

2.3.3 宽带传输

宽带就是指比音频带宽（4kHz）更宽的频带，它包括大部分的电磁波频谱。使用这种宽频带进行传输的系统，称为宽带传输系统。它可以容纳所有的广播，并且可以进行高速率的数据传输。宽带传输允许在同一信道上进行数字信息和模拟信息服务。一个宽带信道可以被划分为多个逻辑信道，这样就能把声音、图像和数据信息综合在一个物理信道中同时进行传输，相互之间不会产生冲突。常见的应用如有线电视系统（CATV）、ISDN 等。

2.3.4 并行通信与串行通信

按照通信中使用的信道数，数据通信方式可分为并行通信和串行通信。

（1）并行（Parallel）通信：数据以成组的方式在多个并行信道上同时传输，如图 2-17 所示。例如，将构成 1 个字符代码的二进制比特位分别在多条并行线路上同时传输，每个比特使用一条单独的线路。并行通信非常普遍，特别是两个短距离的设备之间。最常见的例子是计算机和外围设备之间的通信，如打印电缆。CPU、存储器模块和设备控制器之间的通信也是并行通信。

并行通信应用到长距离的连接时就无优点可言了。首先，在长距离上使用多条线路要比使用一条线路昂贵。另外一个问题涉及比特传输所需要的时间。短距离时，多个信道上同时传输的比特几乎总是能够同时收到。但长距离时，导线上的电阻会或多或少地阻碍比特的传输，从而使它们的到达稍快或稍慢，这将给接收端带来麻烦。

（2）串行（Serial）通信：数据流以串行方式在一条信道上传输，即在一条线路上逐个传送所有的比特，如图 2-18 所示。这种传输方式给发送设备和接收设备增加了额外的复杂性。发送方必须明确比特发送的顺序。例如，在发送一字节的 8 个比特位时，发送方必须确定是先发送高位比特还是先发送低位比特。同样，接收方必须知道一个目标字节中收到的第一个比特位应该放在什么位置上。如果串行通信的双方在比特的顺序上无法取得一致，则数据的传输将出现错误。

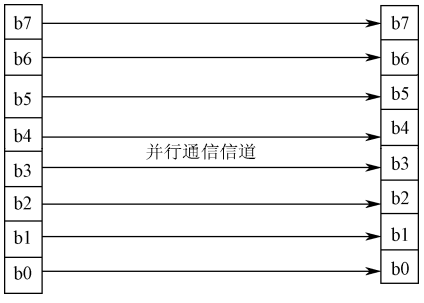


图 2-17 并行通信

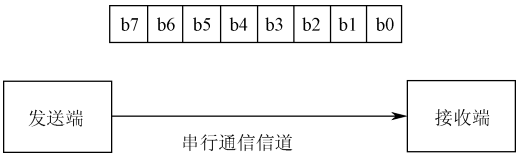


图 2-18 串行通信

由于串行通信的收、发双方只需要有一条传输信道，比较便宜又易于实现，而且用在长距离连接中也比并行通信更加可靠，因此是目前广泛采用的一种方式。在计算机网络中普遍采用串行传输方式。

2.3.5 单工、半双工与全双工通信

（1）单工（Simplex）通信：数据信号只能沿着一个方向传输，发送方只能发送不能接收，接收方只能接收而不能发送，任何时候都不能改变信号传输的方向，如图 2-19（a）所示。例如，无线电广播和电视广播。

（2）半双工（Half-Duplex）通信：数据信号可以沿两个方向传输，但同一时间只允许信号在一个信道上单向传输。因此，半双工通信实际上是一种可切换方向的单工通信，如图 2-19（b）所示。传统的对讲机使用的就是半双工通信方式。

（3）全双工（Full-Duplex）通信：数据信号可以同时沿两个方向传输，在发送数据的同时也可以接收数据，如图 2-19（c）所示。例如我们常用的电话系统就是全双工通信，这种通信方式也适用于计算机之间的通信。

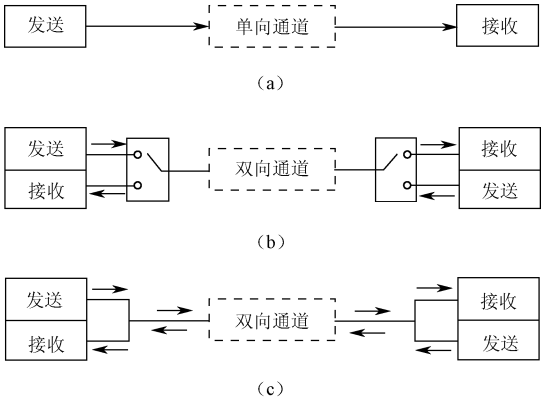


图2-19　单工通信、半双工通信、全双工通信

2.4　多路复用技术

实现在同一条通信线路上传送多路信号的技术称为多路复用技术。电信线路是构成电信网的基础设施之一，在整个电信网的投资中占有很大的比例。“多路复用”可以提高电信传输系统传输能力、扩大容量、挖掘潜力、降低成本。因而无论是有线传输系统还是无线传输系统，都在积极研究开发“多路复用技术”。

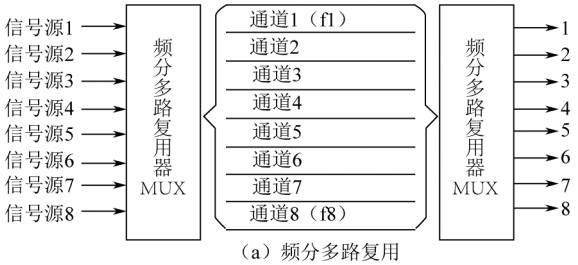
在有线电信方面，早期的传输线路一对线只能传送一路电话，后来发明了载波电话，使上述情况有了突破。单路载波电话在一对线上可以通两路电话，使线路的利用率提高了一倍。后来陆续开发出 3 路、12 路、60 路载波电话等，使电信线路的传输能力提高了几倍、

几十倍。同轴电缆载波系统更使通信的容量从几百路提高到几千路、上万路。20 世纪 70 年代后期，开始大量使用光纤通信。一条光纤就可以通几百上千路电话。到 20 世纪 90 年代中期，一根光纤可以开通几万路电话；人们又研究开发了新的多路复用技术，叫做“波分复用”。现在一根光纤已能开通几十万路电话，而且还在继续迅速提高，其通信容量发展之快令人咋舌，而这些都是“多路复用技术”的成果。

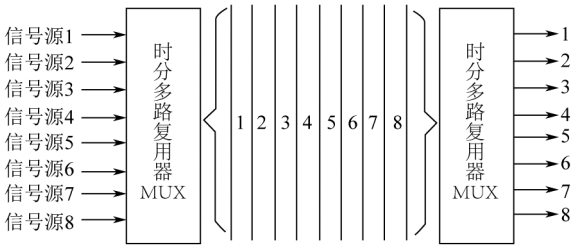
在无线通信方面，多路复用技术也得到广泛的应用。早在 20 世纪 30 年代初期，在无线电通信中就使用了多路复用技术。20 世纪 40 年代以后，微波通信中更是广泛地应用了多路复用技术。到 20 世纪 80 年代，模拟调频微波通信的容量已经高达 1800～2700 路。20 世纪 80 年代末发展起来的数字微波通信，多路复用的容量更高。1965 年以后，卫星通信发展很快，到 20 世纪 90 年代，新的卫星通信系统应用多路复用技术，可以承载约 35000 路电话和多个电视节目的传输。

多路复用技术的基本原理是：各路信号在进入同一个有线的或无线的传输媒质之前，先采用调制技术把它们调制为互相不会混淆的已调制信号，然后进入传输媒质传送到对方，对方再用解调（反调制）技术对这些信号加以区分，并使它们恢复成原来的信号，从而达到多路复用的目的。

常用的多路复用技术有频分多路复用技术和时分多路复用技术。频分多路复用是将各路信号分别调制到不同的频段进行传输，多用于模拟通信。时分多路复用技术是利用时间上离散的脉冲组成相互不重叠的多路信号，广泛应用于数字通信。频分多路复用和时分多路复用的基本原理分别如图 2-20（a）（b）所示。除了频分和时分多路复用技术外，还有一种波分复用技术。这是在光波频率范围内，把不同波长的光波，按一定间隔排列在一根光纤中传送。这种用于光纤通信的“波分复用”技术，现在正在迅速发展之中。



（a）频分多路复用



（b）时分多路复用

图 2-20　频分多路复用和时分多路复用

2.5 数据交换技术

前面讨论的数据通信为最简单形式，即两个使用某种类型的传输介质直接连接的设备之间的通信。但是，在实际环境中，直接连接两个设备往往是不现实的，常常是通过有中间节点的网络来把数据从源点发送到目的点，以此实现通信。这些中间节点一般不会去关 n 心数据的内容，仅仅通过某种交换设备，将数据传向下一个节点直至目的站点。

通常将交换网络中所有通信的发送方与接收方的主机均称为站点，而将通信交换设备称为节点。这些节点以不规则的网状结构用传输线路互相连接起来，而每个站点都连接到某个节点上。

在交换网络中，站点之间需要通过有关节点之间的数据交换才能实现数据通信，通常使用的交换技术有电路交换、报文交换和分组交换。

2.5.1 数据交换的基本概念

数据在通信线路上进行传输的最简单形式，是在两个互联的设备之间直接进行数据通信，但是网络中所有设备都直接两两相连是不现实的，会造成通信系统中的通信介质、设备费用投资相对较大，出于成本考虑，当通信用户数量较多且通信距离较远时，通常要经过中间节点将数据从信源逐点传送到信宿，从而实现两个互连设备之间的通信。中间节点只作为交换设备，把数据从一个节点转发到另一个节点，最终到达接收端。通常将数据在各节点间的数据传输过程称为数据交换。

网络中常用的数据交换技术可分为两大类：电路交换和存储转发交换，其中存储转发交换又可分为报文交换和分组交换。

2.5.2 电路交换

电路交换（Circuit Switching）是在两个站点之间通过通信子网的节点建立一条专用的通信线路，这些节点通常是一台采用机电与电子技术的交换设备（如程控交换机）。也就是说，在两个通信站点之间需要建立实际的物理连接，其典型实例是两台电话之间通过公共电话网络的互联实现通话。

电路交换实现数据通信需经过下列三个步骤：首先是建立连接，即建立端到端（站点到站点）的线路连接；其次是数据传送，所传输数据可以是数字数据，也可以是模拟数据；最后是拆除连接，通常在数据传送完毕后由两个站点之一终止连接。

电路交换的优点是实时性好，但将电话采用的电路交换技术用于传送计算机或远程终端的数据时，会出现下列问题：① 用于建立连接的呼叫时间大大长于数据传送时间，这是因为在建立连接的过程中，会涉及一系列硬件开关动作，时间延迟较长，如某段线路被其他站点占用或物理断路，将导致连接失败，并需重新呼叫；② 通信带宽不能充分利用，效

率低，这是因为两个站点之间一旦建立起连接，就独自占用实际连通的通信线路，而计算机通信时真正用来传送数据的时间一般不到 10%，甚至可低至 1%；③ 由于不同计算机和远程终端的传输速率不同，因此必须采取一些措施才能实现通信，如不直接连通终端和计算机，而设置数据缓存器等。

2.5.3 报文交换

报文交换（Message Switching）是通过通信子网上的节点采用存储转发的方式来传输数据的，它不需要在两个站点之间建立一条专用的通信线路。报文交换中传输数据的逻辑单元称为报文，其长度一般不受限制，可随数据不同而改变。一般它将接收报文站点的地址附加于报文一起发出，每个中间节点接收报文后暂存报文，然后根据其中的地址选择线路再把它传到下一个节点，直至目的站点。

实现报文交换的节点通常是一台计算机，它具有足够的存储容量来缓存所接收的报文。一个报文在每个节点的延迟时间等于接收报文的全部位码所需时间、等待时间，以及传到下一个节点的排队延迟时间之和。

报文交换的主要优点是线路利用率较高，多个报文可以分时共享节点间的同一条通道；此外，该系统很容易把一个报文送到多个目的站点。报文交换的主要缺点是报文传输延迟较长，而且随报文长度变化，不能满足实时或交互式通信的要求，不能用于声音连接，也不适合远程终端与计算机之间的交互通信。

2.5.4 分组交换

分组交换（Packet Switching）的基本思想包括数据分组、路由选择与存储转发。它类似于报文交换，但它限制每次所传输数据单位的长度（典型的最大长度为数千位），对于超过规定长度的数据必须分成若干个等长的小单位，称为分组（Packets）。从通信站点的角度来看，每次只能发送其中一个分组。

各站点将要传送的大块数据信号分成若干等长而较小的数据分组，然后顺序发送；通信子网中的各个节点按照一定的算法建立路由表，即各目标站点各自对应的下一个应发往的节点，同时负责将收到的分组存储于缓存区中，再根据路由表确定各分组下一步应发向哪个节点，在线路空闲时再转发，依此类推，直到各分组传到目的站点。由于分组交换在各个通信路段上传送的分组不大，故只需很短的传输时间（通常仅为毫秒数量级），传输延迟小，故非常适合远程终端与计算机之间的交互通信，也有利于多对时分复用通信线路；此外由于采取了错误检测措施，可保证非常高的可靠性；而在线路误码率一定的情况下，小的分组还可减少重新传输出错分组的费用；与电路交换相比，分组交换带给用户的优点则是费用低。

根据通信子网的不同内部机制，分组交换子网又可分为面向连接（Connect-Oriented）和无连接（Connectless）两类。前者要求建立称为虚电路（Virtual Circuit）的连接，一对主机之间一旦建立虚电路，分组即可按虚电路号传输，而不必给出每个分组的显式目标站点地址，在传输过程中也无须为其单独寻址，虚电路在关闭连接时撤销。后者不建立连接，

数据报（Datagram，即分组）带有目标站点地址，在传输过程中需要为其单独寻址。

分组交换的灵活性高，可以根据需要实现面向连接或无连接的通信，并能充分利用通信线路，因此现有的公共数据交换网都采用分组交换技术。LAN 局域网也采用分组交换技术，但在局域网中，从源站到目的站只有一条单一的通信线路，因此，不需要公用数据网中的路由选择和交换功能。

2.6 差错控制技术

我们理想的计算机网络是可以高速并且没有错误的传输数据，但这种情况基本不可能实现。计算机网络是一个非常复杂的系统，它的诸多组成部分，还有网络在运行时所面临的各种问题都会导致数据传输出现错误。例如在数字数据通信中，由发送器发送的数据信号帧（Frame）在经由网络传到接收器后，由于多种原因可能导致错误位（Bit Errors）的出现。因此能够发现并纠正传输过程中出现的差错就成为了我们必须要解决的问题。

2.6.1 差错控制的基本概念

差错控制就是采取适合的技术手段对传输中出现的错误进行控制，尽可能提高传输的可靠性。常见的方法是发送器向所发送的数据信号帧添加错误检验码，并取该错误检测码作为该被传输数据信号的函数；接收器根据该函数的定义进行同样的计算，然后将两个结果进行比较，如果结果相同，则认为无错误位；否则认为该数据帧存在错误位。

一般来说，错误检测可能出现以下三种结果：

（1）在所传输的数据帧中未探测到，也不存在错误位；

（2）所传输的数据帧中有一个或多个被探测到的错误位，但不存在未探测到的错误位；

（3）被传输的数据帧中有一个或多个没有被探测到的错误位。

显然人们希望尽可能选择好的检测函数，使检测结果可靠，即所有的错误最好都能被检测出来；如检测出现无错结果，则认为不再存在任何未被检测出来的错误。

2.6.2 差错控制的编码

差错控制一般分为检错法和纠错法。检错法是指在传输中仅仅发送足以使接收端检测出差错的附加位，接收端检测到一个差错就要求重新发送数据。检错法只能检测到数据传输过程中有错误发生，却不能纠正这些错误。纠错法是指在传输中发送足够的附加位，使接收端能以很高的概率检测并纠正大多数差错。错误的纠正方法有两种：一种方法是当通过检验码发现有错误时，接收方要求数据的发送方重新发送整个数据单元；另一种方法是采用错误纠正码进行数据传输，自动纠正发生的错误。

理论上，纠错法可以纠正任何一种二进制编码错误。但是错误纠正码比错误检测码要复杂得多，数据的冗余位需要很多。数据单元传输过程中发生的错误有三种：单位错误、多位错误和突发错误。纠正多位错误和突发错误所需要的位数很大，在大多数情况下，纠

错的效率低下。因此，大多数的纠错技术都局限于一位、两位或三位的错误。目前，汉明码是一种常用的错误纠正编码技术。

差错控制方式基本上分为两类，一类称为“反馈纠错”；另一类称为“前向纠错”。在这两类基础上又派生出一类称为“混合纠错”。

1．反馈纠错

这种方式是指发信端采用某种能发现一定程度传输差错的简单编码方法对所传信息进行编码，加入少量监督码元，在接收端则根据编码规则对收到的编码信号进行检查，一旦检测出有错码，即向发信端发出询问信号，要求重发。发信端接收到询问信号时，立即重发已经发生传输差错的那部分信息，直到正确收到为止。所谓发现差错，是指在若干接收码元中知道有一个或一些是错的，但不一定知道错误的准确位置。

2．前向纠错

这种方式是指发信端采用某种在解码时能纠正一定程度传输差错的较复杂的编码方法，使接收端在收到的信元中不仅能发现错码，还能够纠正错码。采用前向纠错方式时，不需要反馈信道，也不需反复重发而延误传输时间，对实时传输有利，但是纠错设备比较复杂。

3．混合纠错

混合纠错是指少量错误在接收端自动纠正，差错较严重、超出自行纠正能力时，就向发信端发出询问信号，要求重发。因此，“混合纠错”是“前向纠错”和“反馈纠错”两种方式的混合。

2.6.3 差错控制方法

实际采用的错误检测方法主要有两类：奇偶校验（Parity）和 CRC 循环冗余校验。

对数据信号帧传输过程中的位错进行修正的方法主要有以下两种：

（1）由发送器提供错误修正码，然后由接收器自己修正错误；

（2）在接收器发现接收到的错误帧中有位错误时，通知发送器重新发送数据信号帧。

第一种方法中的错误修正码需要发送器由被传送数据信号帧计算得到，然后添加到数据帧的后面，其长度几乎等于数据位数，导致效率降低 50%，实际采用不多；一般采用较为有效的第二种重发送方法。

习　题　2

一、填空题

1．通信的目的是为了_____。信息的载体可包含语音、音乐、图形、图像、文

字和数据等多种媒体。

2．信道按传输信号的形式可分为_____和_____。

3．数据通信系统的基本组成一般包括发送端、_____以及收发两端之间的_____三个部分。

4．码元是对于网络中传送的_____数字中每一位的通称，也常称为“位”或 bit。

5．调制速率 *B* 是脉冲信号经过调制后的传输速率，以_____（Baud）为单位，通常用于表示调制器之间传输信号的速率。

6．按照通信中使用的信道数，数据通信方式可分为_____和_____。

7．数据通信方式按照信号传送方向与时间的关系，可分为_____、_____和_____三种方式。

8．在模拟信道中，常用带宽表示信道传输信息的能力，带宽即传输信号的_____与_____之差。

9．波特率指数据信号对载波的调制速率，它用单位时间内载波调制状态_____来表示，其单位为波特（Baud）。

10．传输介质分为_____和_____两大类。

11．RJ-45 接口采用透明塑料材料制作，由于其外观晶莹透亮，常被称为“_____”。

12．根据光在光纤中的传播方式，光纤分为两种类型，即_____和_____。

13．常见的无线传输介质有_____、_____、_____等。

14．_____成本相对比较低，目前已经被广泛地应用于长途电话、蜂窝电话、电视转播等场合。

15．在信道中直接传送基带信号时，称为_____。

16．具有调制和解调功能的装置称为_____，即 MODEM。

17．实现在同一条通信线路上传送多路信号的技术称为_____技术。

18．并行传输适用于数据的_____传输，串行传输适用于数据的_____传输。

二、选择题

1．如果一个码元所承载的信息量是 4 位，则这一码元可以表示的状态为（　　）。

A．4　　B．8

C．16　　D．32

2．信息在信道中传输，传送的形式必须是（　　）。

A．数据　　B．信息

C．信号　　D．码元

3．我们平时说话的声音属于（　　）数据。

A．模拟　　B．数字

C．混合　　D．复合

4．数据传输的基本单位是（　　）。

A．bit　　B．Byte

C．数据字　　D．数据块

5．数据传输速率在数值上等于每秒传输构成数据代码的二进制比特数，它的单位为比特/秒，通常记作（　　）。

A．B/s　　B．bps

C．bpers　　D．baud

6．信息传输的物理通道是（　　）。

A．信道　　B．介质

C．编码　　D．数据

7．用电话线进行通信，适合使用（　　）方式。

A．单工　　B．半双工

C．并行通信　　D．串行通信

8．网络中常用的有线介质是（　　）。

A．双绞线　　B．同轴电缆

C．光纤　　D．微波

9．常用的 UTP 线是（　　）。

A．双绞线　　B．同轴电缆

C．屏蔽双绞线　　D．非屏蔽双绞线

10．当需要用线缆将计算机与交换机相连接时，应选用的线缆是（　　）。

A．直通缆　　B．交叉缆

C．全反缆　　D．三者都可

11．双绞线的两根绝缘铜导线按一定密度互相绞合在一起的目的是（　　）。

A．阻止信号的衰减　　B．降低信号的干扰程度

C．增加数据的安全性　　D．没有任何作用

12．根据（　　），可以将光纤分为单模光纤和多模光纤。

A．光纤的传输速率　　B．光纤的粗细

C．光在光纤中的传播方式　　D．传输距离

13．在下列传输介质中，使用 RJ-45 水晶头作为连接器的是（　　）。

A．双绞线　　B．同轴电缆

C．光纤　　D．无线介质

14．下面的（　　）传输介质的带宽最宽，信号衰减最小，抗干扰性最强。

A．非屏蔽双绞线　　B．屏蔽双绞线

C．光纤　　D．微波

15．下列关于无线传输介质特性的说法中，错误的是（　　）。

A．无线传输介质不通过物理连接，而是通过空间传输的技术

B．微波通信的工作效率很高，沿直线传播

C．红外线适用于长距离传输，能穿透墙壁

D．激光有很好的聚光性和方向性，但是不能穿透雨和浓雾

16．计算机与计算机外设间的数据传输一般是（　　）。

A．宽带传输　　B．无线传输

C．基带传输　　D．频带传输

三、简答题

1．信息与数据有何区别与联系？
2．何为信道？如何分类？如何在模拟信道上传输数字信号？
3．串行通信与并行通信的区别是什么？
4．单工通信与双工通信的区别是什么？
5．数据通信中的主要技术指标有哪些？
6．什么是带宽？
7．屏蔽双绞线（STP）与非屏蔽双绞线（UTP）有何区别？
8．简述单模光纤与多模光纤的区别。
9．常见的无线传输介质如红外线、无线电波、微波各适用什么场合？
10．多路复用技术是什么样的技术？
11．什么是数据交换？常用的数据交换技术有哪些？

第3章 计算机网络体系结构

内容摘要

- 网络体系结构的基本概念
- 网络协议
- 网络的分层结构
- 网络的体系结构
- OSI 参考模型
- TCP/IP 模型

学习目标

- 掌握网络通信协议的概念与特点
- 理解网络的分层结构
- 理解参考模型 OSI
- 熟悉网络各层的功能
- 理解 TCP/IP 协议的工作机制
- 了解 OSI 参考模型与 TCP/IP 模型的差异

随着计算机网络的不断发展和完善，它逐渐涉及了人们生产、生活的各个方面。那么如何最大程度地发挥计算机网络的作用，更好地实现资源共享、数据通信等功能，我们必须解决在计算机网络中面临的诸多问题，包括信号的传输、差错的控制、路由寻址、数据交换和提供用户接口等。计算机网络体系结构就是我们为简化对上述问题的研究、设计与实现而构建出的一种结构模型。

计算机的网络结构可以从网络体系结构、网络组织和网络配置三个方面来描述。网络组织是从网络的物理结构和网络的实现两方面来描述计算机网络；网络配置是从网络应用方面就计算机网络的布局、硬软件和通信线路来描述计算机网络；网络体系结构是从功能上来描述计算机网络结构，阐述的是计算机网络功能实体的划分原则及相互之间协同工作

的方法和规则。

3.1 网络体系结构的基本概念

为了减少计算机网络的复杂程度，按照结构化设计方法，计算机网络将其功能划分为若干个层次，较高层次建立在较低层次的基础上，并为其更高层次提供必要的服务功能。网络中的每一层都起到隔离作用，使得低层功能具体实现方法的变更不会影响到高层所执行的功能。

网络体系结构是指能完成计算机间的通信合作，把每个计算机互联的功能划分成有明确定义的层次，并规定同层次进程通信的协议及相邻层之间的接口服务；也即指用分层研究方法定义的网络各层的功能，各层协议和接口的集合。

协议是通信双方所做的一种需要共同遵守的约定，没有协议通信几乎不可能完成。通信的问题很复杂，因此，导致通信协议也很复杂。在 IT 技术中，凡是复杂的问题都应该模块化、层次化，协议是个软件，软件编程可以分层，分层后各层子协议完成通信的不同功能，化整为零，最后完成通信的整个功能。分层的方法及各层子协议的集合被称为协议的体系结构，目前有多种不同的体系结构，如 SNA、DNA、ARPANET、IPX/SPX 等，因此，需要制定体系结构的标准。

很多标准化组织开始致力于体系结构标准的制定，最著名的是由 ISO 制定的 OSI 开放系统互联参考模型，但 OSI 并没有形成产品。TCP/IP 协议是 Internet 上采用的协议，虽然不是体系结构的标准，但是一个广泛使用的工业产品，是一个工业标准，是事实上的标准。

3.1.1 网络协议

协议是通信双方共同遵守的约定，是用来描述进程之间信息交换过程的一组术语。在计算机网络中包含有多种计算机系统，它们的硬件和软件系统有着很大的差异，要使得它们之间能够相互通信，进行数据交换，就必须有一套通信管理机制使通信双方能正确地接收信息，并能理解对方的信息含义，它们必须事先约定一个规则，这种规则就称为协议。

1．通信协议

协议是一组规则的集合，是进行交互的双方必须遵守的约定。在网络体系中，为了保证数据通信双方能正确而自动地进行通信，针对通信过程的各种问题，制定了一整套约定，这就是网络系统的通信协议。

网络通信协议主要由 3 个要素组成：语法、语义和交换规则。语法是以二进制形式表示的命令和相应的结构，确定协议元素的格式（规定数据与控制信息的结构和格式）；语义是由发出请求、完成的动作和返回的响应组成的集合，确定协议元素的类型，即规定通信双方要发出何种控制信息、完成何种动作以及做出何种应答；交换规则规定事件实现顺序的详细说明，即确定通信状态的变化和过程，如通信双方的应答关系。

下面以日常生活中的甲打电话给乙为例来说明协议的概念。

甲有事情需要与乙联系，就打电话给乙，甲首先拿起电话拨通乙的电话号码，乙方电话振铃，乙拿起电话，此时通话开始，通话完毕后，双方挂断电话，完成通信联系。在这个过程中，甲方与乙方都遵守了打电话的协议。其中，电话号码就是“语法”的一个例子，一般的电话号码由若干位的阿拉伯数字组成；甲拨通乙的电话后，乙的电话就会振铃，振铃是一个信号，表示有电话打进，乙选择接电话，这一系列的动作包括了控制信号、响应动作等，就是“语义”；甲拨了电话，乙的电话才会响，乙听到铃声后才会考虑要不要接，这一系列事件的因果关系十分明确，不可能没有人拨乙的电话而乙的电话会响，也不可能在电话铃没响的情况下，乙拿起电话却从话筒中传出甲的声音，这就是“交换规则”。

从上面的例子可以看出协议是使两个不同实体能够实现通信而制定的一些规范。如在上例中双方如何建立通话联系、如何交换、何时通信等。

2．通信协议的特点

（1）层次性。由于网络系统体系结构是有层次的。通信协议被分为多个层次，在每个层次内又可以被分成若干子层，协议各层次有高低之分。

在计算机网络术语中，层就是一个或一系列的程序，能为相邻的更高层提供服务，同时使用相邻低层提供的服务。位于最高层的程序为用户提供高级的服务，它要依靠低层为其提供信息和传送消息。

（2）可靠性和有效性。如果通信协议不可靠就会造成通信混乱和中断，只有通信协议有效，才能实现系统内的各种资源共享。

3.1.2 网络的分层结构

计算机网络系统的功能强、规模庞大，通常采用高度结构化的分层设计方法，将网络划分为一组功能分明、相对独立和易于操作的层次，依靠各层之间的功能组合提供网络的通信服务，从而减少网络系统设计、修改和更新的复杂性。

在现实社会中，有时会遇到很多复杂、庞大的问题或任务。如何有效地在短时间内进行处理，通常会将任务分解为一个个小的任务，降低统一处理的难度。如图 3-1 所示以日常生活中的邮政系统为例说明任务的分解情况。

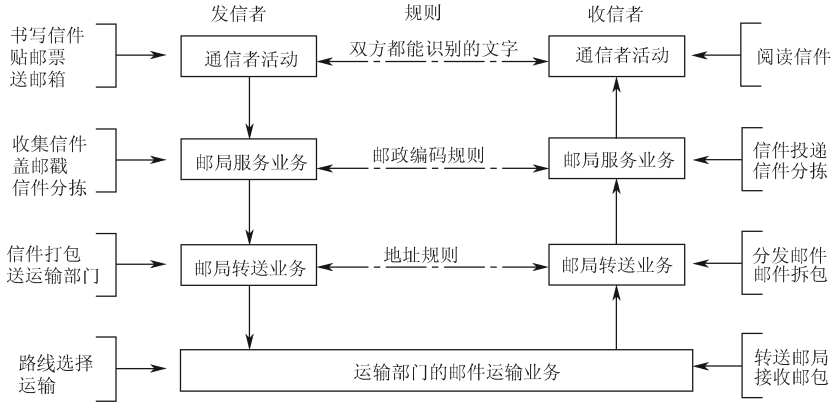


图 3-1　邮政系统模型

从如图 3-1 所示的流程框图可以看到，一个人给另外一个人寄信的过程是一个很繁杂的过程，但如果把这个过程分为很多的层次，把任务分配出去，每个层次只需要负责好自己的任务，大家协作就可以按部就班地完成这个任务。

计算机网络是一个涉及通信系统和计算机系统的复杂系统。为了降低系统设计和实现的难度，把计算机网络要实现的功能进行结构化和模块化的设计，将整体功能分为几个相对独立的子功能层次，各个功能层次间进行有机的连接，下层为其上层提供必要的功能服务。分层可将庞大而复杂的问题转化为若干较小的局部问题，这些较小的局部问题就比较容易研究和处理了。这种层次结构的设计称为网络层次结构模型，如图 3-2 所示。

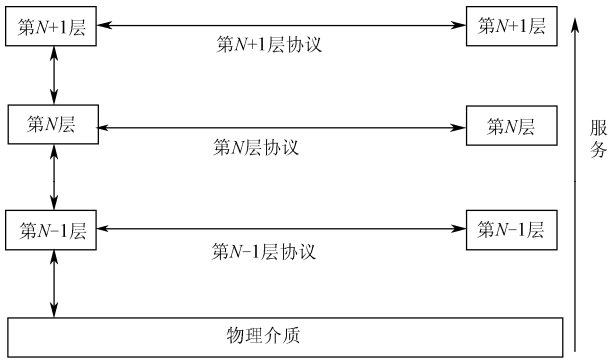


图 3-2　网络层次结构模型

在网络层次结构模型中，N 层是 N–1 层的用户，同时又是 N+1 层的服务提供者。对 N 层而言，N+1 层用户直接获得了 N 层提供的服务，而 N 层的服务是建立在 N–1 层所提供的服务基础之上的。

一台计算机上的第 N 层与另一台计算机上对应的第 N 层进行对话，通话的规则就是第 N 层协议。实际上数据并不是从一台计算机上的第 N 层直接传送到另一台计算机上的第 N 层，而是每一层都把数据和控制信息交给它的下一层，直到最下层，最后由物理层完成实际的数据通信。

网络体系结构中采用层次化结构的优点如下。

（1）各层之间相互独立，高层不必关心低层的实现细节，只要知道低层所提供的服务，以及本层向上层所提供的服务即可，能真正做到各司其职。

（2）有利于实现和维护，某个层次实现细节的变化不会对其他层次产生影响。

（3）易于实现标准化。

分层时每一层的功能应非常明确，层数不宜太多，否则会给描述和综合实现各层功能和系统工程任务带来较多的困难，但层数也不能太少，不然会使每一层的协议太过复杂。

3.1.3　网络的体系结构

20 世纪 70 年代以后，随着计算机网络的逐渐普及，随之而来的是不同体系之间的计算机网络的连接显得非常的复杂。每个计算机网络厂商都有自己的网络模型，网络模型使得该厂商的计算机之间能够方便地通信，这种情况显然有利于计算机网络厂商对市场的垄断，用户一旦使用了某个厂商的网络，就只能全部购买该厂商的网络产品，如果购买了其他厂商的产品，由于分属不同的网络模型，相互之间就很难连通。当时世界上最大的两家计算机厂商是国际商业机器公司（International Business Machines，IBM）和数字设备公司（Digital Equipment Corporate，DEC）。IBM 制定了自己的网络模型，称为系统网络体系结构（System Network Architecture，SNA）。DEC 也建立了自己的网络模型，称为 DECnet。两个模型的设

计都非常优秀，但是分别按照不同模型搭建好的计算机网络之间是不能相互通信的。

想象一下，如果相同的情况发生在电话上，如果你给你的朋友打电话，对方使用的是另一家厂商的电话，你们俩将无法通话。因此，网络的发展迫切需要一个能互联互通的标准，各网络设备厂商就可以遵照共同的标准来开发网络产品，最终实现彼此兼容。

3.2　OSI 参考模型

1983 年国际标准化组织 ISO 正式颁布了网络体系结构标准——开放系统互联参考模型 OSI/RM（Open System Interconnection/Reference Model），简称 OSI，形成了所谓七层协议的体系结构。OSI 参考模型对于计算机网络的发展有着十分深远的影响，包括像 TCP/IP 这样的协议，都从它那里吸取有价值的成分，它提示了组成网络各组件的内在联系，提示了网络运行的根本原理。

OSI/RM 并不是一个具体的网络，它只给出了一些原则性的说明，规定了开放系统的层次结构和各层所提供的服务。它将整个网络的功能划分为 7 个层次，而且在两个通信实体之间的通信必须遵循这 7 层协议，如图 3-3 所示。

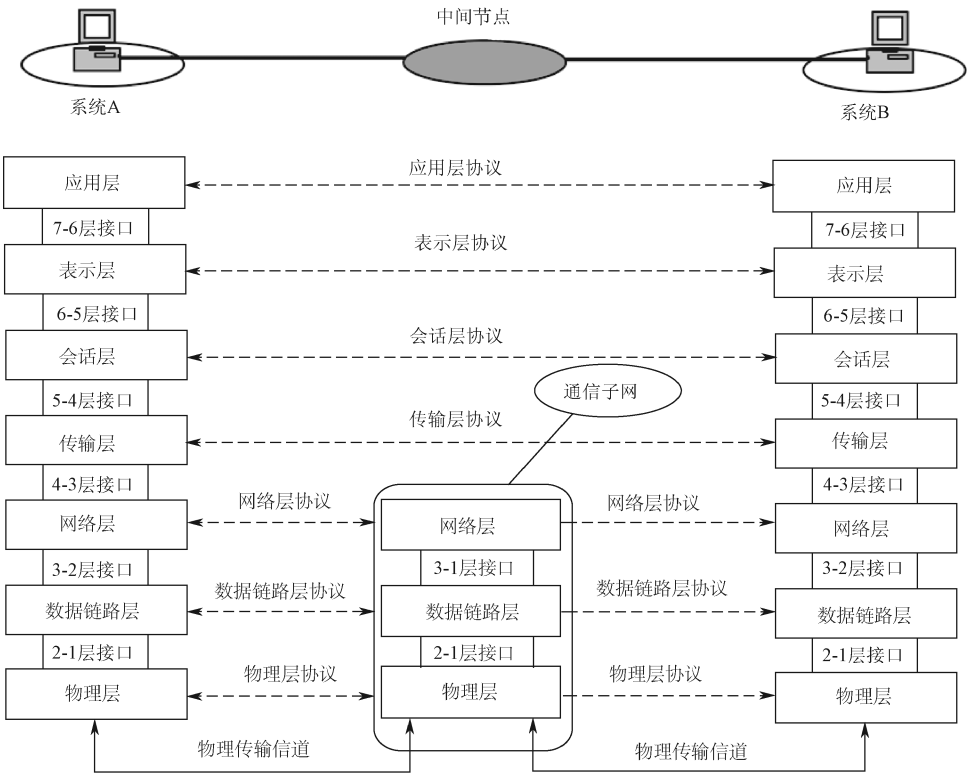


图 3-3　OSI 参考模型示意图

OSI/RM 从下向上的 7 个层次分别为物理层、数据链路层、网络层、传输层、会话

层、表示层和应用层。最高层为应用层，面向用户提供服务；最低层为物理层，连接通信媒体实现数据传输。层与层之间的联系是通过各层之间的接口来进行的，上层通过接口向下层提出服务请求，而下层通过接口向上层提供服务。两个用户计算机通过网络进行通信时，除物理层之外，其余各对等层之间不存在直接的通信关系，而是通过各对等层的协议来进行通信。只有两个物理层之间才通过媒体进行真正的数据通信。在实际应用中，两个通信实体是通过一个通信子网进行通信的，一般来说，通信子网中的节点只涉及低 3 层的结构。

3.2.1 OSI 参考模型简介

OSI 参考模型将网络分为 7 个层次，其中第一层到第三层属于通信子网的功能范畴，第五层到第七层属于资源子网的范畴，第四层起着衔接上下三层的作用。各层在网络中发挥着各自的作用。

OSI 参考模型的成功之处在于，它清晰地区分了服务、接口和协议这三个容易混淆的概念，服务描述了每一层的功能，接口定义了某层提供的服务和如何被高层访问，而协议是每一层功能的实现方法。

综上所述，可以分析出该模型具有以下特点。

（1）每层的对应实体之间都通过各自的协议进行通信。

（2）各个计算机系统都有相同的层次结构。

（3）不同系统的相应层次具有相同的功能。

（4）同一系统的各层次之间通过接口联系。

（5）相邻的两层之间，下层为上层提供服务，上层使用下层提供的服务。

3.2.2 物理层

物理层处于 OSI 参考模型的最低层，直接面向网络传输介质；物理层负责将二进制数据位流（bit）通过传输介质，从一台计算机发送给另一台计算机。物理层不关心具体数据位流的具体含义。物理层完全面向硬件，定义了物理结构和传输介质的电气机械规格，包括电压、通信速率、最大传输距离、物理连接器和其他类似的属性等。

物理层具体解决了以下问题。

（1）使用什么类型的传输介质，使用什么样的连接器件和连接设备。

（2）使用什么类型的拓扑结构。

（3）使用什么样的物理信号表示二进制的 0 和 1，以及该物理信号与传输相关的特性如何。

在常用的网络设备中，集线器工作在 OSI 参考模型的物理层，因为物理层处理的是位（bit），所以集线器的作用也就是重发位，将所收到的位信号进行再生和还原并传给每个与之相连的网段。集线器是一个没有鉴别能力的设备，它会转发所收到的位信号，也包括错误信号。

3.2.3 数据链路层

数据链路层位于 OSI 参考模型的第二层，位于物理层的上方和网络层的下方。物理层实现了位流的传输，但是此传输并不是可靠的数据通信。数据链路层就在物理层的基础上，通过将位组织封装成帧，从而建立一条可靠的数据传输通道。

数据帧是用来传输数据的一种结构包，这个结构包中除了有所传输数据的实际数据外，还包括发送端和接收端的网络地址以及控制信息和错误校验信息。通过网络地址，确定了数据将去往何处，通过控制信息和错误校验信息检查传输数据是否有误，如果有错误帧存在，则要求重发该帧。

数据链路层具体解决了以下问题。

（1）将位信息加以组织封装成帧。

（2）确定了数据帧的结构。

（3）通过使用硬件地址及物理地址来寻址。

（4）实现差错校验信息的组织。

（5）对共享的介质实现访问控制。

在常用的网络设备中，网卡是工作在物理层和数据链路层重要的网络设备，网卡在发送端把系统要发送过来的数据转换成能在介质上传输的位流，在接收端，把从介质接收的位流重新组成计算机系统可以处理的数据。同时，每块网卡都由生产厂商固化了一个全球唯一的物理地址，也就是 MAC 地址，它由 48 个二进制数组成，通常用 12 个十六进制数来表示，如 00:e0:4c:01:02:85 或者 00-e0-4c-01-02-85，其中前 6 个十六进制数代表网络硬件制造商编号，由 IEEE 组织分配，后 6 个十六进制数代表序列号，由生产厂商分配。在数据链路层通信时，使用 MAC 地址可以实现发送与接收。

交换机是工作在数据链路层的网络设备，交换机具有物理寻址功能，交换机启动以后，通过学习，逐渐在内存中建立一个 MAC 地址与交换机端口的关联表，从而实现有目的的数据转发。

3.2.4 网络层

网络层位于 OSI 参考模型的第三层，位于数据链路层的上方和传输层的下方。通信通过寻址和路由选择为发送端和接收端连接一个或多个数据传输的链路。在网络层，提供了数据的网络地址，也就是 IP 地址，同时提供了统一的寻址方案，因此它屏蔽了底层的技术细节，把各种网络统一到了一个逻辑平台上。网络层传输的数据单位称为分组。

网络层具体解决了以下问题。

（1）提供了网络层的地址（IP 地址），并进行不同网络系统间的路径选择。

（2）数据包的分割和重新组合。

（3）差错校验和恢复。

（4）流量控制和拥塞控制。

路由器是工作在 OSI 参考模型的网络层的重要设备，通过网络层的地址路由器可以为

网络访问提供访问路径。路由器同时在数据传输过程中实现流量控制和差错管理。

3.2.5 传输层

传输层位于 OSI 参考模型的第四层，位于网络层的上方和会话层的下方。传输层负责准确可靠地将数据从网络的一端传到另一端。下面三层提供的数据并不是完全可靠的，传输层加强数据的传输服务，可以将下面三层的无连接或不受保护的通信升级为更可靠的通信。

传输层具体解决了以下问题。

（1）建立连接。

（2）保证数据无差错地传输。

3.2.6 网络高层

1．会话层

会话层位于 OSI 参考模型的第五层，位于传输层的上方和表示层的下方。会话层主要负责管理远程用户或进程之间的通信。

会话层具体解决了以下问题。

（1）会话的建立。

（2）通信的控制。

2．表示层

表示层位于 OSI 参考模型的第六层，位于会话层的上方和应用层的下方。表示层确保一个系统的应用层发送的信息能够被另一个系统读取。也就是完成数据格式之间的转换。表示层将数据进行转换和翻译，从而使发送端和接收端都能够理解。

表示层具体解决了以下问题。

（1）数据的表示。

（2）数据的压缩与解压。

（3）定义传输的句法和转换。

3．应用层

应用层处于 OSI 参考模型的顶层，直接面向用户；它为数据库访问、电子邮件、文件传输等用户应用程序提供直接服务。应用层可实现网络中一台计算机上的应用程序与另一台计算机上的应用程序之间的通信。例如，发送端和接收端都使用 MSN 进行聊天时，应用层就将 MSN 通信时所需要的数据得到，并交给下层处理，完成通信。

应用层具体解决了以下问题。

（1）提供用户接口，得到传输的数据。

（2）提供面向用户的界面，即实用程序，使得用户可以利用这些程序完成实际的工作。

（3）涉及网络服务、服务公告及服务使用方式。

在 OSI 参考模型中各层完成各层的功能，各层的功能细化起来比较复杂，但各层的基本功能如图 3-4 所示。

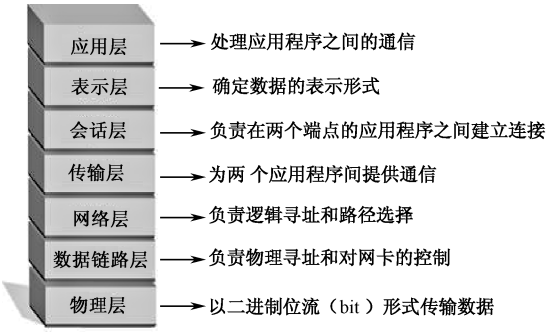


图 3-4　各层的基本功能

3.3　TCP/IP 模型

TCP/IP 协议起源于 20 世纪 70 年代，当时的 ARPA 为了实现异种机异种网之间的互联，大力资助网间网技术的开发与研究，1973 年，斯坦福大学的两名研究人员提出了 TCP/IP 协议。TCP/IP 是一组协议，其中 TCP 和 IP 是两个重要的协议。TCP 是传输控制协议，提供面向连接的服务，IP 是网际互联协议，提供无连接数据报服务和网际路由服务。

3.3.1　TCP/IP 层次结构

TCP/IP 协议把整个网络协议分为 4 个层次：网络接口层、网络互联层、传输层和应用层。它们都建立在硬件基础上，如图 3-5 所示为 TCP/IP 的层次结构。

3.3.2　TCP/IP 体系结构中各层的功能

1．网络接口层

TCP/IP 模型的最低层是网络接口层，也被称为网络访问层。在 TCP/IP 模型中没有详细定义这一层的功能，只是指出通信主机必须采用某种协议连接到网络上，并且能够传输网络数据分组。具体是哪种协议，在本层里没有规定，它包括了能使用 TCP/IP 与物理网络进行通信的协议。实际上根据主机与网络拓扑结构的不同，局域网基本上采用了 IEEE 802 系列的协议，如 IEEE 802.3 以太网协议、IEEE 802.5 令牌环网协议；广域网常采用的协议有 PPP、帧中继、X.25 等。

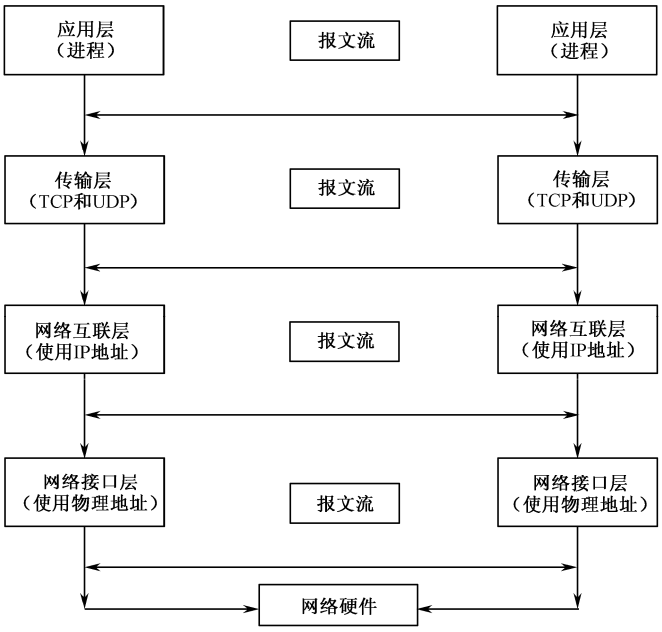


图 3-5　TCP/IP 的层次结构

2．网络互联层

网络互联层是在 Internet 标准中正式定义的第一层。网络互联层主要功能是负责在互联网上传输数据分组。网络互联层与 OSI 参考模型的网络层相对应。相当于 OSI 参考模型中网络层的数据报服务。

网络互联层是 TCP/IP 模型中最重要一层，它是通信的枢纽，从低层来的数据包要由它来选择继续传给其他网络节点或是直接交给传输层，对从传输层来的数据包，要负责按照数据分组的格式填充报头，选择发送路径，并交由相应的线路发送出去。

在网络互联层，主要定义了网络互联协议，即 IP 协议及数据分组的格式。本层还定义了地址解析协议 ARP、反向地址解析协议 RARP 及网际控制报文协议 ICMP。

3．传输层

TCP/IP 的传输层也被称为主机至主机层，它主要负责端到端的对等实体之间进行通信。它与 OSI 参考模型的传输层功能类似，也对高层屏蔽了底层网络的实现细节，同时它真正实现了源主机到目的主机的端到端的通信。该层使用了两种协议来支持数据的传送，它们是 TCP 协议和 UDP 协议。

TCP 协议是可靠的、面向连接的协议。它用于包交换的计算机通信网络、互联系统及类似的网络上，保证通信主机之间有可靠的字节流传输。

UDP 协议是一种不可靠的、无连接协议。它最大的优点是协议简单、效率较高，额外开销小，缺点是不能保证正确的传输，也不排除重复信息的发生。

4．应用层

在 TCP/IP 模型中，应用程序接口是最高层，它与 OSI 模型中的高三层的任务相同，都是用于提供网络服务，如文件传输、远程登录、域名服务和简单网络管理等。目前，互联网上常用的应用层协议主要有以下几种。

（1）简单邮件传输协议（SMTP）：主要负责互联网中电子邮件的传递。

（2）超文本传输协议（HTTP）：提供 Web 服务。

（3）远程登录协议（Telnet）：实现对主机的远程登录功能，常用的电子公告牌系统 BBS 使用的就是这个协议。

（4）文件传输协议（FTP）：用于交互式文件传输。

（5）域名解析（DNS）：实现逻辑地址（IP 地址）到域名地址的转换。

3.3.3 两个重要的协议

TCP/IP 不是一个简单的协议，而是由一组小的、专业化协议构成的，包括 TCP、IP、UDP、ARP、ICMP，以及其他的许多被称为子协议的协议。在众多的子协议中，IP 和 TCP 协议是最重要的核心协议。

1．IP 协议

IP 协议属于 TCP/IP 模型的网络互联层，其基本任务是通过互联网传输数据报，提供关于数据应如何传输以及传输到何处的信息，各个数据报之间是互相独立的。IP 是一种使 TCP/IP 可用于网络连接的子协议，可以跨越多个局域网段或通过路由器跨越多种类型的网络，在一个网际环境中，连接在一起的单个网络被称为子网，使用子网是 TCP/IP 联网的一个重要部分。

IP 所在的网络互联层通过网络接口层与物理网络接口。在局域网中网络接口层通常为网络接口设备驱动程序。IP 协议主要承担了在网际进行数据报无连接的传送、数据报寻址和差错控制，向上层提供 IP 数据报和 IP 地址，并以此统一各种网络的差异性（不同的网络，其帧结构不同）。

IP 协议借助中间的一个或多个 IP 网关，实现从源网络到目的网络的寻径。源网络为信源机的网络，目的网络为信宿机的网络。当 IP 数据报到达目的网络所连的网关时，目的网络借助网络层中的地址解析协议 ARP 对目的主机进行寻址。

在互联网中，IP 网关是一个十分重要的网际部件，其主要功能为“存储—寻址—转发”。它对传输层及其以上层次的功能并不关心，上层信息只是封装在 IP 数据报的数据部分中，与反映 IP 层功能的 IP 数据报的报头部分毫不相干。

在通信子网中，各网关的低四层间传输的是基于分组的数据报，从源网关到目的网关中间经过的路径（网关）并不固定。由于网际是动态的（例如中间某一网关的开关或损坏等），每经过一个中间网关都存在“存储—寻址—转发”等问题。源网关和目的网关间不存在一条固定的连接通道，所以数据报提供的总是“无连接”的服务。按照 TCP/IP 的设计思想，认为数据传输的可靠性问题应由传输层（TCP 协议）来解决，处于 IP 层的各中间网关

不处理可靠性问题，网络层的主要责任是尽快地把 IP 数据报从信源机传递到信宿机，IP 数据报在传递途径中可能出错、重复或消失。

2．TCP 协议

传输控制协议 TCP 属于 TCP/IP 协议群中的传输层，是一种面向连接的子协议，在该协议上准备发送数据时，通信节点之间必须建立起一个连接，才能提供可靠的数据传输服务。TCP 协议位于 IP 协议的上层，通过提供校验、流控制及序列信息来弥补 IP 协议可靠性上的缺陷。

TCP 是一种面向连接的协议，在面向连接的环境中，开始传输数据之前，在两个终端之间必须先建立一个连接。建立连接的过程可以确保通信双方在发送数据报之前已准备好了传送和接收数据。对于一个要建立的连接，通信双方必须采用彼此的初始化序列号 seq 和来自对方成功传输确认的应答号 ack 来同步（ack 号指明希望收到的下一个 8 位组的编号）。将同步信号写为 SYN，应答信号写为 ACK。三次握手的过程如图 3-6 所示。

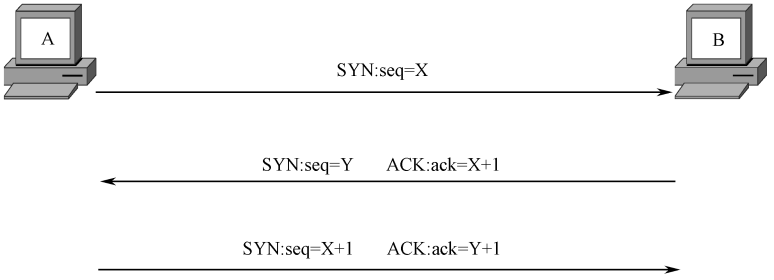


图 3-6 三次握手的过程

① 主机 A 发送一个同步标志信号 SYN 给主机 B：初始化序列号 seq 是 X。

② 主机 B 发送 SYN、ACK 给主机 A：序列号 seq 是 Y，应答号 ack 是 X＋1。

③ 主机 A 发送 SYN、ACK 给主机 B：序列号 seq 是 X＋1，应答号 ack 是 Y＋1。

通过以上三个步骤（三次握手），TCP 连接建立，开始传送数据。

处于通信子网和资源子网之间的传输层利用网络层提供的不可靠的、无连接的数据报服务，向上层提供可靠的面向连接的服务。为了提高网络服务的质量，保证可靠性高的数据传输，TCP 必须提供如下的功能。

① 提供面向连接的进程通信。进行通信的双方在传输数据之前，首先必须建立连接，数据传输完成之后，任何一方都可以根据自己的情况断开连接。TCP 建立的连接是点到点的全双工连接，在建立连接之后，通信双方可以同时进行数据的传输。

② 提供差错检测和恢复机制。由于 TCP 协议之下的 IP 层只提供了简单的分组服务，所以传输过程中可能出现各种错误情况，如数据报可能因为拥塞或线路故障而丢失，在同一次会话中的不同数据报经过了不同的路由，而使数据报的接收顺序与发送顺序不一致等。所以 TCP 要实现差错恢复和排序等功能。

TCP 使用滑动窗口机制来实现差错控制，它对每一个传输的字节进行编号，每个分段中的第一字节的序号随该分段进行传输，每个 TCP 分段中还带有一个确认号，表示接收方

希望接收的下一字节的序号。在 TCP 传输了一个数据分段后，把该分段的一个备份放入重新传输队列中并启动一个时钟，如果在时钟超过之前得到对该分段的确认，则从队列中删除该分段，如果没有收到确认，则重新传输该分组。

③ 流量控制机制。在 TCP 中通过动态改变滑动窗口的大小，实现流量控制。窗口的大小表示在最近收到的确认号之后允许传送的数据长度，如果窗口大小为 0，则表示当前的接收方没有能力接收另外的数据，必须等待新的确认信息改变窗口大小。此外，TCP 还可以检测网络拥塞情况，并且根据它调整数据发送速率。

3．其他协议

除了 IP 协议和 TCP 协议外，传输层和网络互联层还有一些重要的协议在发挥各自不同的作用，这些协议主要有用户数据报协议（UDP）、网际控制报文协议（ICMP）、地址解析协议（ARP）以及反向地址解析协议（RARP）。

（1）用户数据报协议（UDP）

用户数据报协议位于 TCP/IP 模型的传输层中，它是一种无连接的传输服务，不能保证数据报以正确的序列被接收，不提供错误校验和序列编号。然而通过 Internet 进行实况录音或电视转播时，要求迅速发送数据时，UDP 的不精确性使得它比 TCP 协议更加有效、更有用，在这种情况下，具有验证、校验，以及流量控制机制的 TCP 协议将增加太多的报头，使得其发送延迟。

（2）网际控制报文协议（ICMP）

ICMP 位于 TCP/IP 模型网络互联层的 IP 协议和 TCP 协议之间，它不提供差错控制服务，而是仅仅报告哪一个网络是不可到达的，哪一个数据报因分配的生存时间过期而被抛弃。常用于诊断实用程序中，如 Ping、Tracert。

（3）地址解析协议（ARP）

地址解析协议是一个网络互联层协议，用于实现 IP 地址到 MAC 地址（物理地址）的转换。它获取主机或节点的物理地址并创建一个本地数据库以便将物理地址映射到主机 IP 地址中。

（4）反向地址解析协议（RARP）

网络互联层还有一个反向地址解析协议，用于实现物理地址到 IP 地址的转换，主要用于网上的无盘工作站。网络上的无盘工作站在网卡上有自己的物理地址，但不知道自己的 IP 地址，为了能根据物理地址找出 IP 地址，在网络上至少要设置一个 RARP 服务器，网络管理员必须事先把网卡上的物理地址和相应的 IP 地址加入 RARP 数据库中。无盘工作站是经过广播一个 RARP 请求包给网络上的所有主机来寻找自己的 IP 地址，再由网络上的 RARP 服务器给予响应。

3.3.4 OSI 参考模型与 TCP/IP 模型的比较

OSI 参考模型与 TCP/IP 模型都采用了层次结构，但 OSI 采用的是 7 层模型，而 TCP/IP 是 4 层结构；前者主要针对广域网，很少考虑网络互联问题，后者从一开始就注意到网络互联技术，并最终促成了席卷全球的 Internet。

TCP/IP 模型的网络接口层实际没有真正定义，其功能相当于 OSI 模型的物理层与数据链路层，事实上，就是物理网络的物理层与数据链路层。TCP/IP 的网络互联层相当于 OSI 参考模型中网络层中的无连接网络服务。OSI 模型与 TCP/IP 模型的传输层功能基本相似，都是负责为用户提供真正的端到端的通信服务，对高层屏蔽了低层网络的实现细节。所不同的是，TCP/IP 模型的传输层是建立在网络互联层基础之上的，而网络互联层只提供无连接的服务，所以面向连接的功能完全在 TCP 协议中实现，当然 TCP/IP 的传输层还提供无连接的服务，如 UDP；OSI 模型的传输层是建立在网络层基础之上的，网络层既提供面向连接的服务，又提供无连接服务，但传输层只提供面向连接的服务。在 TCP/IP 模型中，没有会话层和表示层，事实证明，这两个层次的功能可以完全包含在应用层中。

3.3.5 IP 地址

为了在网络环境下实现计算机之间的通信，网络中的任何一台计算机必须有一个地址，而且同一个网络中的地址不允许重复。一般情况下在网络上任何两台计算机之间进行数据传输时，所传输的数据开头必须包括某些附加信息，这些附加信息中最重要的是发送数据的计算机地址和接收数据的计算机地址。

IP 地址是互联网上为每一台主机分配的由 32 位二进制数组成的唯一标识符，就像人们平常所说的家庭地址或单位地址一样，有了这个地址其他人才可能找到。每台计算机在网络中有了 IP 地址，其他计算机才能与其进行通信。

1．IP 地址的概念

网络通信需要每个参与通信的实体都具有相应的地址，地址一般符合某种编码规则，并用一个字符串来标识一个地址，不同的网络可以具有不同的编址方案，现在网络中广泛使用的是 IP 地址。

所谓 IP 地址，就是给每一个接入网络的计算机的主机分配的网络地址，这个地址在公网上是唯一的，在单位内部的网络中，每台主机的地址也必须是唯一的，否则会出现地址冲突的现象。目前 IP 地址使用的是 32 位的 IPv4 地址，它是 32 位的无符号二进制数，分为 4 个字段，以×.×.×.×表示，每个×为 8 位，对应的十进制取值为 0～255。

IP 地址由网络地址和主机地址两部分组成，如图 3-7 所示。其中，网络地址用来标识一个物理网络，主机地址用来标识这个网络中的一台主机。

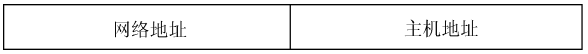


图 3-7　IP 地址的结构

例如，给出一个用二进制表示的 IP 地址：11001001.00001101.00110010.00000011，每个字段对应的值分别是：201、13、50、3。因此，一个完整的 IP 地址可用小数点表示法表示成：201.13.50.3。

IP 地址的结构使网络的寻址分两步进行：① 路由器先按 IP 地址中的网络地址把网络找到；② 找到目的网络后，再用 ARP 协议找到主机。由于一台主机可能有多个 IP 地址，

因此 IP 地址只是标识了一台计算机的某个接口。

2．IP 地址的分类

IP 地址采用的是 32 位的二进制数来表示，理论上可以支持 2^{32} 台主机，也就是约 40 多亿台主机。为了更好地对这些 IP 地址进行管理，同时适应不同的网络需求，根据 IP 地址的网络位所占的位数的不同，互联网地址授权委员会（IANA）将 IP 地址分为以下几类，如图 3-8 所示。

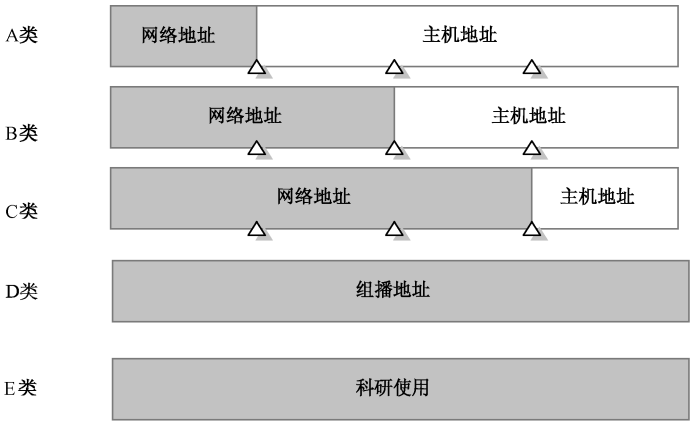


图 3-8　IP 地址分类

A 类 IP 地址中的第一个 8 位组表示网络位，其余三个 8 位组表示主机地址。A 类地址使每个网络拥有的主机数量非常多。A 类地址的第一个 8 位的第一位总是被设置为 0，这也就限制了 A 类地址的第一个 8 位组的值始终小于 127。

B 类 IP 地址中的前两个 8 位组表示网络位，后两个 8 位组表示主机地址。同时 B 类地址的第一个 8 位的前两位总是被设置为 10，所以 B 类地址的第一段的范围为 128～191。

C 类 IP 地址中的前三个 8 位组表示网络位，后一个 8 位组表示主机地址。同时 C 类地址的第一个 8 位的前三位总是被设置为 110，所以 C 类地址的第一段的范围为 192～223。

D 类地址用于 IP 网络中的组播，它不像 A、B、C 类地址有网络号和主机号，同时 D 类地址的第一个 8 位的前 4 位总是被设置为 1110，所以 D 类地址的第一段的范围为 224～239。

E 类地址被留作科研实验使用，而其第一个 8 位的前 4 位为 1111，所以 D 类地址的第一段的范围为 240～255。

各类 IP 地址网络号字段与主机号字段的关系，如图 3-9 所示。

可以看出 A 类地址的结构使每个网络拥有的主机数非常多，而 C 类地址拥有的网络数目很多，每个网络所拥有的主机数却很少。这样就说明了 A 类地址多为大型网络所使用，而 C 类地址支持的是大量的小型网络，各类 IP 地址的网络地址数与主机地址数如表 3-1 所示。

3．特殊的 IP 地址

IP 地址除了可以表示主机的一个物理连接外，还有几种特殊的表现形式，这些特殊的 IP 地址作为保留地址，从不分配给主机使用。

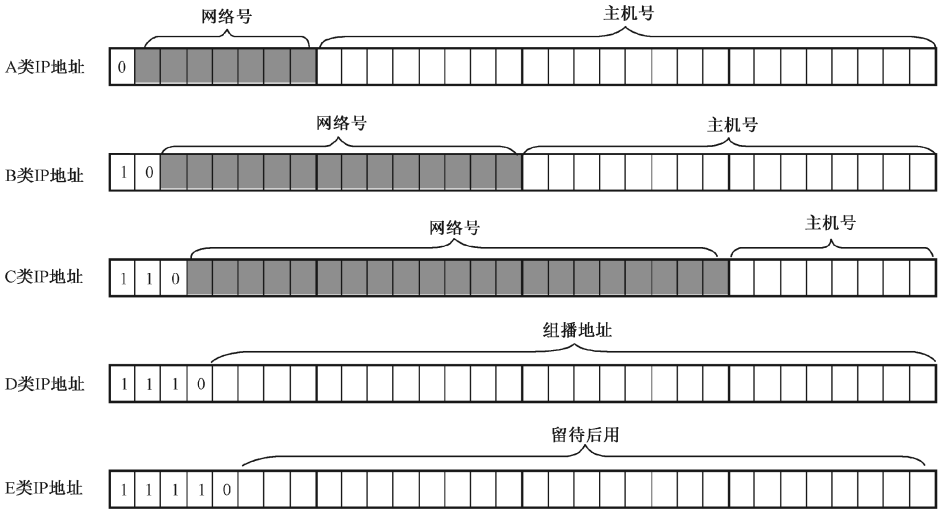


图 3-9　各 IP 地址网络号字段和主机号字段的关系

表 3-1　各类 IP 地址网络地址数与主机地址数

地址类型	引导位	第一段的范围	地址结构	可用网络地址数	可用主机地址数
A类	0	1～126	网. 主. 主. 主	126(2^7–2)	16777214(2^{24}–2)
B类	10	128～191	网. 网. 主. 主	16383(2^{14}–1)	65534(2^{16}–2)
C类	110	192～223	网. 网. 网. 主	2097151(2^{21}–1)	254(2^8–2)
D类	1110	224～239	组播地址		
E类	1111	240～255	研究和实验用地址		

（1）网络地址

在互联网中经常需要使用网络地址，那么怎样表示一个网络呢？IP 地址方案中规定网络地址是由一个有效的网络号和一个全“0”的主机号构成的。例如，在 A 类网络中，地址 120.0.0.0 就表示该网络的网络地址；B 类网络中，地址 180.10.0.0 就表示该网络的网络地址；C 类网络中，地址 202.80.120.0 就表示该网络的网络地址。

（2）广播地址

当一个设备向网络上所有的设备发送数据时，就产生了广播。为了能使网络上所有设备能够注意到这样一个广播，广播地址要有别于其他的 IP 地址，通常这样的 IP 地址以全“1”结尾。

IP 广播地址有两种形式：直接广播和有限广播。

① 直接广播。如果广播地址包含一个有效的网络号和一个全“1”的主机号，技术上称为直接广播地址。在互联网中任意一台主机均可以向其他网络进行直接广播。

例如，C 类地址 202.80.120.255 就是一个直接广播地址。网络中的一台主机如果使用该 IP 地址作为数据报的目的 IP 地址，那么这个数据报将同时发送给 202.80.120.0 网络上的所有主机。

② 有限广播。IP 地址的 32 位全为“1”（255.255.255.255）用于本地广播，该地址称为有限广播地址。有限广播将广播限制在最小的范围内，如果采用标准 IP 编址，那么有限广播将被限制在本网络之中，如果采用子网编址，有限广播将被限制在本子网中。

（3）回送地址

A 类网络地址 127.0.0.0 是一个保留地址，用于网络软件测试以及本地计算机进程间通信。这个 IP 地址称为回送地址。无论什么程序，一旦使用回送地址发送数据，协议软件不进行任何网络传输，立即将之返回。因此，含有网络号 127 的数据报不可能出现在任何网络上。

（4）专用 IP 地址

专用 IP 地址是在所有 IP 地址中专门保留的三个区域的 IP 地址，这些地址不在公网上分配，专门留给用户组建内部网络使用，也称为私有 IP 地址。这三个区域分别属于 A、B 和 C 类地址空间的 3 个地址段，这些地址可以满足任何规模的企业和机构的应用，其地址范围如表 3-2 所示。

表 3-2　专用 IP 地址范围

地　址　段	主 机 位 数	IP 地址个数
10.0.0.0～10.255.255.255	24 位	2^{24}，约 1700 万个
172.16.0.0～172.31.255.255	20 位	2^{20}，约 100 万个
192.168.0.0～192.168.255.255	16 位	2^{16}，约 6.5 万个

4．IP 地址分配原则

使用 IP 地址必须遵循一些原则，并且一些 IP 地址被用于特殊的 TCP/IP 通信，任何时候都不能使用。

（1）只有 A、B、C 三类地址可以分配给计算机和网络设备；

（2）IP 地址的第一段不能为 127，保留作测试使用；

（3）网络地址不能全为 0，也不能全为 1。全为 0 表示主机地址，全为 1 用做网络掩码；

（4）主机地址不能全为 0，也不能全为 1。全为 0 表示网络地址，全为 1 代表广播地址；

（5）IP 地址在网络中必须唯一。

3.3.6　子网与子网掩码

在互联网中，A 类、B 类和 C 类 IP 地址是经常使用的 IP 地址，经过网络号和主机号的划分，它们能适应不同的网络规模。但仅靠 A、B、C 类网络地址来划分网络会有许多问题，如 A 类地址和 B 类地址都允许一个网络中包含大量的主机，如表 3-3 所示。但实际上不可能将这么多主机连接到一个单一的网络中，这不仅会降低互联网地址的利用率，还会给网络寻址和管理带来很大的困难。所以在实际应用中，通过在网络中引入子网解决这个问题。

表 3-3　IP 地址的使用范围

网 络 类 型	最大网络数	第一个可用网络号	最后一个可用网络号	每个网络中最大主机数
A	126	1	126	16777214
B	16383	128.1	191.255	65534
C	2097151	192.0.1	223.255.255	254

1．子网

A 类网络包含了多于 1600 万个 IP 地址，B 类网络包含了多于 65000 个 IP 地址。单独来看，这个数字已经比较大了。如果你考虑将这么多台计算机放在一起来工作，你就知道这样的网络管理的难度是多大了。现在含有数百台设备的局域网已经不多见了，而包含有上千台设备的单个局域网就更少见了。如果你使用一个 A 类或 B 类的网络来连接一个局域网，那么必将会有很多的 IP 地址没有使用。实际工作中，可以采用将网络切割成多个小的网络的方法来解决这个问题。将网络内部划分成多个部分，各部分单独工作，在互联网文献中，这些部分称为子网。

2．子网掩码

子网掩码（Subnet Mask）又称为网络掩码或地址掩码，是一种用来指明一个 IP 地址的哪些位标识的是主机所在的子网，以及哪些位标识的是主机位的掩码。子网掩码不能单独存在，它必须结合 IP 地址一起使用。在 IP 地址中，网络地址和主机地址是通过子网掩码来分开的。每个子网掩码是一个 32 位的二进制数，一般由两部分组成，前一部分使用连续的“1”用来标识网络地址，后一部分使用连续的“0”用来标识主机地址。

例如，对于一个 IP 地址为 131.110.133.15 的主机，由于是处于 B 类网络中，因此在默认情况下，用户应该将此 IP 地址配合使用的子网掩码设置为 11111111　11111111　00000000　00000000，表示网络地址为 16 位，主机地址为 16 位，用十进制数表示就是 255.255.0.0。各类网络的默认子网掩码如下：

A 类　11111111　00000000　00000000　00000000，十进制数表示为 255.0.0.0

B 类　11111111　11111111　00000000　00000000，十进制数表示为 255.255.0.0

C 类　11111111　11111111　11111111　00000000，十进制数表示为 255.255.255.0

子网掩码的主要作用是将网络地址从 IP 地址中剥离出来，求出 IP 地址的网络号。使用 IP 地址与子网掩码进行“与”运算所得出的结果就是网络地址。有了网络号后，就可以判断应如何发送数据报了。每台主机在数据报发送前，都要通过子网掩码判断是否应将数据报发往路由器。TCP/IP 将目标 IP 与本机子网掩码求与，得出目标主机网络号，将目标主机网络号与本机网络号进行比较，看看是否相等，如果相等则说明目标主机就在本子网内，应直接将数据报发送给目标主机，如果不等则说明目标主机不在本网络内，则应将数据报发送给路由器。

将 IP 地址和它的子网掩码相结合，就可以判断出 IP 地址中哪些位表示网络和子网，哪些位表示主机。

例如，给出一个经过子网编址的 B 类 IP 地址 131.110.133.15，并不知道在子网划分时到底借用了几位主机号来表示子网，但是当给出了它的子网掩码 255.255.255.0 后，如图 3-10

所示，就可以根据与子网掩码中的“1”相对应的位表示网络的规定，得到该子网划分借用了 8 位来表示子网，并且该 IP 地址所处的子网号为 133。

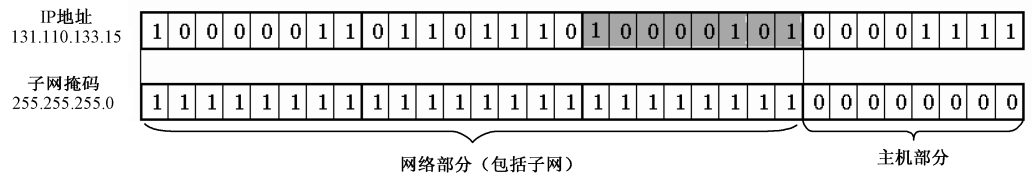


图 3-10　借用 B 类地址的 8 位表示子网

如果借用该 B 类 IP 地址的 5 位主机号来划分子网，如图 3-11 所示，那么它的子网掩码为 255.255.248.0，IP 地址 131.110.133.15 所处的子网号为 16。

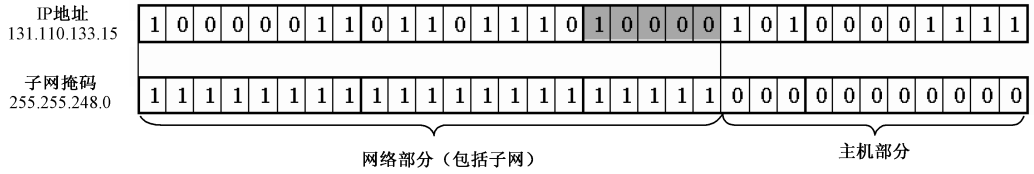


图 3-11　借用 B 类地址的 5 位表示子网

3．子网设计

设从主机标志部分借用 n 位给子网，剩下 m 位作为主机标志位，那么生成的子网数量为 2^n-2，每个子网具有的主机数量为 2^m-2 台。设计的基本过程如下：

（1）根据所要求的子网数和主机数量公式 2^n-2 推算出 n。n 应是一个最小的接近要求的正整数。

（2）求出相应的子网掩码，即用默认掩码加上从主机标志部分借出的 n 位组成新的掩码。

（3）子网的部分写成二进制，列出所有子网和主机地址，去除全“0”和全“1”地址。

例 1　一个 C 类地址 192.168.2.0/26，请问该网络可以划分为几个子网？每个子网可容纳多少台主机？

这是一个 C 类网络，正常情况下，主机是 8 位，网络位是 24 位，子网掩码全 1 位是 24 位。而本例的子网掩码全 1 位为 26 位，说明网络位从主机位借了 2 位地址用于子网的编址，子网掩码的点分二进制表示法为：

11111111 . 11111111 . 11111111 . 11000000，即 255.255.255.192

由于是 C 类地址，所以主机标志位原为 8 位，现从中借出了 2 位，即 n=2。

那么，m=8–2=6。

依据上面的分析，可得出子网数为 2^2-2=2 个；

每个子网的主机数为 2^6-2=62 台。

例 2　某网络的地址为 192.168.132.0，网内有 252 台主机。为了管理需要，要将该网络分成 6 个子网，每个子网能容纳 30 台主机。请给出子网掩码和对应的地址空间。

这是一个 C 类网络，正常情况下，主机是 8 位，网络位是 24 位，子网掩码全 1 位是 24 位。本例要求将网络分为 6 个子网，每个子网中能够容纳 30 台主机。

2^5=32>30，也就是说主机位只需要有 5 位就可以了。主机位可以借出 3 位给网络位，2^3–2=6，正好满足 6 个子网的要求。子网掩码的长度为 24+3=27 位，子网掩码的最后一个字节就是 11100000，该网络的子网掩码为 255.255.255.224。

IP 地址空间的规划如表 3-4 所示。子网部分写成二进制，列出所有子网和主机地址，并去除全“0”和全“1”。

表 3-4　IP 地址空间的规划表

子 网 号	主机地址 1	主机地址 2	主机地址 3	…	主机地址 31	主机地址 32
	00000	00001	00010	…	11110	11111
000	0	1	2	…	30	31
001	32	33	34	…	62	63
010	64	65	66	…	94	95
011	96	97	98	…	126	127
100	128	129	130	…	158	159
101	160	161	162	…	190	191
110	192	193	194	…	222	223
111	224	225	226	…	254	255

表 3-3 中给出的是子网部分的 IP 地址分配情况，主机地址与子网号交叉的单元即该子网内的一个 IP 地址的最后一字节的二进制值。例如，子网号“010”与主机地址 2 交叉的单元，取值为“65”，该 IP 地址为 192.168.132.65。表中，对应每个子网，分别包含 2^5=32 个 IP 地址。子网号为“000”和“111”的两行，主机地址为“00000”和“11111”的两列均需要排除，所以实际可用的子网划分情况如下：

001 子网　　对应的地址范围：192.168.132.33～192.168.132.62

010 子网　　对应的地址范围：192.168.132.65～192.168.132.94

011 子网　　对应的地址范围：192.168.132.97～192.168.132.126

100 子网　　对应的地址范围：192.168.132.129～192.168.132.158

101 子网　　对应的地址范围：192.168.132.161～192.168.132.190

110 子网　　对应的地址范围：192.168.132.193～192.168.132.222

例 3　网络为 172.30.0.0，每个子网需要容纳 700 台主机，请问子网掩码该如何设置？

这是一个 B 类网络，正常情况下，主机是 16 位，网络位是 16 位，子网掩码全 1 位是 16 位。本例对网络进行分割，每个子网中能够容纳 700 台主机。

$$2^9=512<700<1024=2^{10}$$

所以 m=10；网络号–子网号=32–10=22；子网掩码长度为 22，网络位向主机位借了 6 位用于网络编址，子网掩码为 11111111 . 11111111 . 11111100 . 00000000，对应的子网掩码为 255.255.252.0。

例 4　网络为 172.19.0.0，子网掩码为 255.255.248.0，请问该网络可以划分为几个子网？每个子网有多少个有效 IP 地址？

由网络地址可知，这是一个 B 类网络，默认子网掩码为 255.255.0.0。现在其子网掩码为 255.255.248.0，将 248 转换为二进制为 11111000，可知网络位从主机位借了 5 位划分子网，即 n=5，m=16–5=11。

所以，划分的子网数为 2^5–2=30 个；每个子网有效 IP 数为 2^{11}–2=2046。

在实际工作中，可以按照表 3-5 和表 3-6 所示进行子网的划分，以及子网掩码的设置。

表 3-5　C 类网络子网划分关系表

子网位数	子网掩码	子网数	主机数
2	255.255.255.192	2	62
3	255.255.255.224	6	30
4	255.255.255.240	14	14
5	255.255.255.248	30	6
6	255.255.255.252	62	2

如果选择 B 类网络，可以按照表 3-6 所示的子网位数、子网掩码、可容纳的子网数和主机数的对应关系进行子网规划与划分。

表 3-6　B 类网络子网划分关系表

子网位数	子网掩码	子网数	主机数
2	255.255.192.0	2	16382
3	255.255.224.0	6	8190
4	255.255.240.0	14	4094
5	255.255.248.0	30	2046
6	255.255.252.0	62	1022
7	255.255.254.0	126	510
8	255.255.255.0	254	254
9	255.255.255.128	510	126
10	255.255.255.192	1022	62
11	255.255.255.224	2046	30
12	255.255.255.240	4094	14
13	255.255.255.248	8190	6
14	255.255.255.252	16382	2

习　题　3

一、填空题

1. 在网络层次结构模型中，N 层是 N–1 层的_____，同时又是 N+1 层的_____。对 N 层而言，N+1 层用户直接获得了 N 层提供的_____。

2. 一台计算机上的第 N 层与另一台计算机上对应的第 N 层进行对话，通话的规则就是

_____。

3．在网络体系中，为了保证_____能正确而自动地进行通信，针对通信过程的各种问题，制定了一整套_____，这就是网络系统的通信协议。

4．网络通信协议主要由 3 个要素组成：_____、_____和交换规则。

5．语法是以二进制形式表示的命令和相应的结构，规定_____与_____的结构和格式。

6．开放系统互联参考模型简称_____，是由_____组织在 20 世纪 80 年代初提出来的。

7. OSI/RM 从下向上的 7 个层次分别为_____、_____、_____、_____、_____、_____和_____。最高层为应用层，面向_____提供服务；最低层为物理层，面向_____实现数据传输。

8．物理层的主要功能有_____、_____和_____。

9．数据链路层的主要功能有_____、_____、_____、_____、_____、_____。

10．数据链路层中传送的数据块被称为_____。

11．数据链路层协议可以分为_____和_____两大类。

12．网络层主要完成_____、_____、_____、_____等功能。

13．网络层提供的服务主要有_____和_____两大类。

14．TCP/IP 将网络分为_____、_____、_____、_____ 4 个层次。

15．TCP/IP 模型应用层的主要协议有_____、_____、_____和_____。

16．IP 协议属于 TCP/IP 模型的_____层，其基本任务是通过_____传输数据报，提供关于数据应如何传输以及传输到何处的信息，各个数据报之间是互相独立的。

17. IP 地址包括_____和_____两部分，可以分为_____类。

18．传输控制协议 TCP 属于 TCP/IP 协议群中的_____，是一种面向_____的子协议，在该协议上准备发送数据时，通信节点之间必须建立起一个_____，才能提供可靠的数据传输服务。

19. 地址解析协议是一个网络互联层协议，用于实现_____到_____的转换。

20．IP 地址由_____和_____两部分组成。其中，_____用来标识一个物理网络，_____用来标识这个网络中的一台主机。

21．子网掩码又称为网络掩码、地址掩码，是一种用来指明一个_____的哪些位标识的是主机所在的_____，以及哪些位标识的是_____的掩码。

二、选择题

1．在网络协议中，涉及数据和控制信息的格式、编码及信号电平等的内容属于网络协议的（　　）要素。

A．语法　　B．语义　　C．定时　　D．语用

2．OSI 体系结构定义了一个（　　）层的模型。

A．8　　B．9　　C．6　　D．7

3．在 OSI 的模型中，主要功能是在通信子网中实现路由选择的是（　　）。

A．物理层　　B．网络层　　C．数据链路层　　D．传输层

4．在 OSI 的模型中，主要功能是组织和同步不同主机上各种进程间通信的层次的是（　　）。

A．会话层　　B．网络层　　C．表示层　　D．传输层

5．在 OSI 的模型中，主要功能是为上层用户提供共同数据或信息语法表示转换，也可以进行数据压缩和加密的层次是（　　）。

A．会话层　　B．网络层　　C．表示层　　D．传输层

6．在开放系统互联参考模型中，把传输的比特流划分为帧的层次是（　　）。

A．网络层　　B．数据链路层　　C．传输层　　D．分组层

7．在计算机网络中，允许计算机相互通信的语言被称为（　　）。

A．协议　　B．寻址　　C．轮询　　D．对话

8．在 OSI 模型中，提供建立、维护和拆除物理链路所需的机械的、电气的、功能的和规程的特性的层次是（　　）。

A．网络层　　B．数据链路层　　C．物理层　　D．传输层

9．物理层的基本作用是（　　）。

A．规定具体的物理设备

B．规定传输信号的物理媒体

C．在物理媒体上提供传输信息帧的逻辑链路

D．在物理媒体上提供传输原始比特流的物理连接

10．数据链路层中的数据块常被称为（　　）。

A．信息　　B．分组　　C．比特流　　D．帧

11．TCP 通信建立在面向连接的基础上，TCP 连接的建立采用（　　）次握手的过程。

A．1　　B．2　　C．3　　D．4

12．ISO 的中文名称是（　　）。

A．国际认证　　B．国际标准化组织

C．国际指标　　D．国际经济组织

13．Internet 采用的通信协议是（　　）。

A．FTP　　B．SPX/IPX　　C．TCP/IP　　D．WWW

14．在 TCP/IP 环境中，如果以太网上的站点初始化后，只有自己的物理地址而没有 IP 地址，则可通过广播请求，征求自己的 IP 地址，负责这一服务的协议是（　　）。

A．ARP　　B．RARP　　C．ICMP　　D．IP

15．以下 IP 地址中可作为主机 IP 地址的是（　　）。

A．210.223.198.0　　B．220.193.277.81

C．189.210.255.255　　D．109.77.255.255

16．默认情况下子网掩码 255.255.255.0 代表（　　）网络。

A．A 类　　B．B 类　　C．C 类　　D．D 类

17．下列选项中合法的 IP 地址是（　　）。

A．210.2.233　　B．115.123.20.245

C．101.3.305.77　　D．202.38.64.255

18．一般来说，TCP/IP 模型中的 IP 协议提供的服务是（　　）。

A．传输层服务　　B．网络层服务

C．表示层服务　　D．会话层服务

三、简答题

1．简述通信协议的特点。

2．网络体系结构采用层次化的优点是什么？

3．OSI 参考模型和 TCP/IP 模型的共同点和不同点是什么？

4．简述 OSI 网络层的主要功能。

5．什么是子网？使用其的目的是什么？

6．TCP/IP 体系结构中各层的功能是什么？

7．简述 IP 协议的功能。

8．简述 TCP 协议的功能。

9．一个网络子网掩码为 255.255.255.248，该网络能够连接多少主机？

10．IP 地址 192.168.9.101 的默认的子网掩码是什么？

11．一个 C 类地址为 192.9.200.13，其子网掩码为 255.255.255.240，请问在其中每一个子网上的主机数量最多有多少？

12．简述 IP 地址是如何分类的。

第4章 局域网技术

内容摘要

- 局域网概述
- IEEE 802 标准
- 介质访问控制方法
- 局域网的组成
- 局域网的工作模式
- 典型局域网
- 交换式局域网

学习目标

- 掌握局域网的概念与特点
- 理解介质访问控制方法
- 掌握局域网的组成与结构
- 熟悉不同模式局域网的工作方式与特点
- 熟悉典型局域网的特性与应用
- 理解交换式局域网的工作原理与特性

局域网（LAN）是计算机网络的重要组成部分，是当今计算机网络技术应用与发展非常活跃的一个领域。公司、企业、政府部门及住宅小区内的计算机都通过 LAN 连接起来，以达到资源共享、信息传递和数据通信的目的。而信息化进程的加快，更是刺激了通过 LAN 进行网络互联需求的剧增。因此，理解和掌握局域网技术也就显得很重要。

局域网的发展始于 20 世纪 70 年代，至今仍是网络发展中的一个活跃领域。到了 20 世纪 90 年代，LAN 更是在速度、带宽等指标方面有了更大进展，并且在 LAN 的访问、服务、管理、安全和保密等方面有了进一步的改善。例如，Ethernet 技术从传输速率为 10Mbps 的 Ethernet 发展到 100Mbps 的高速以太网，并继续提高至千兆位（1000Mbps）以太网、万兆

位以太网。

4.1 局域网概述

局域网是小型计算机和微型计算机普及与推广之后发展起来的，是目前应用最为广泛的一种重要的基础网络。技术是计算机网络技术中较成熟的技术，也是计算机网络技术中发展最为迅速的技术，由于局域网具有组网灵活、成本低、应用广泛、使用方便、技术简单等特点，已经成为当前计算机网络技术领域中最活跃的一个分支。

4.1.1 局域网的概念与特点

早期的计算机网络大多是广域网，在 20 世纪 80 年代，由于微型计算机的出现，计算机逐渐进入各行各业以及普通家庭。由于微型计算机的大量使用，对处于一栋大楼或位于一个部门内的人们来说，相互之间通过计算机进行信息交换和资源共享的需求越来越迫切，局域网技术就在这种情况下出现了。局域网的名字本身就隐含了这种网络在地理范围上的局域性。正是由于网络的覆盖范围较小，故局域网与广域网在技术等方面存在着一定的差别。

1．局域网的概念

由于局域网技术发展迅速，所以很难给局域网下一个确切的定义。通常认为，局域网是最基本的计算机网络形式，是指在有限的地理区域内构建的计算机网络，按照 IEEE 对“LAN”所下的定义：局域网是一个允许很多彼此独立计算机在适当的区域内、以适当的传输速率直接进行沟通的数据通信系统。

2．局域网的主要特点

局域网通常被限制在中等规模的地理区域内，采用具有较高的数据传输速率和较低误码率的物理通信信道。具体来说，局域网络具有以下主要特点。

（1）局域网覆盖的地理范围小，如一个房间、一幢大楼、一个工厂、一所学校、一个社区，其地理覆盖范围一般在几米到数十千米之间。

（2）通信速率较高。局域网具有较高数据传输速率，一般不小于 10Mbps，以目前的技术来看，速率可达 10000Mbps。

（3）传输延时小、误码率低。局域网数据传输质量高，因为传输距离较短，可使用高质量的传输介质，因而传输的延时小，大约在 1ms 之内；局域网误码率一般在 10^{-9}～10^{-12} 之间，可靠性高。

（4）局域网通常为一个单位所有，是专用网络，便于管理。由于局域网的小范围分布和高速传输，使它适用于对一个部门或一个单位的管理。这样，局域网的所有权可以归某一个单位所有，为单位内部使用，它不需要由国家通信部门参与管理。

（5）便于安装和维护，可靠性高。局域网的安装比较简单，扩充也很容易，在大量

采用的星型局域网中，可以随时增加站点，而且，在某些站点出现故障时，整个网络可以正常工作。局域网可以构成分布处理系统，故障站点的计算任务可以移至其他站点进行处理。

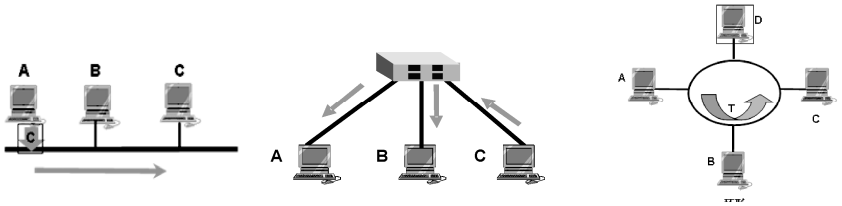
（6）影响局域网特性的主要技术因素是传输介质、拓扑结构和介质访问控制方法。

（7）如果采用宽带局域网，则可以实现对数据、语音和图像的综合传输；在基带网上，采用一定的技术，也有可能实现语音和静态图像的综合传输，可以为办公自动化提供数据传输上的支持。

（8）协议简单、结构灵活、建网成本低、周期短。协议只涉及通信子网的内容，局域网协议模型只包含 OSI 参考模型低三层（通信子网）的内容，但其介质访问控制比较复杂，所以局域网的数据链路层分为 LLC 子层和 MAC 子层。局域网地理范围小，通信线路短，网络设备相对较少，因此节省网络成本，缩短建网周期。

4.1.2 常见的局域网拓扑结构

从应用的观点来看，在中小型局域网中常用到的网络拓扑结构有总线型拓扑结构、星型拓扑结构和环型拓扑结构三种，如图 4-1 所示。



（a）总线型　　（b）星型　　（c）环型

图 4-1　常见的局域网拓扑结构

4.1.3 局域网的体系结构

计算机网络体系结构包含两个方面的内容，一方面是指所有计算机网络都遵照的协议参考模型，另一方面是指一个具体计算机网络所使用的协议栈。在局域网中同样有一个体系结构，也就是它的参考模型。不过它是专门针对局域网的。

按照 IEEE 802 标准，局域网的体系结构由三层协议构成，即物理层（Physical，PHY）、媒体访问控制层（Media Access Control，MAC）和逻辑链路控制层（Logical Link Control，LLC）。

“媒体访问控制层”和“逻辑链路控制层”这两层相当于 OSI 七层参考模型中的第二层，即数据链路层。

在局域网参考模型中，同样每个实体都需要与另一个系统的同等实体按协议进行通信。在一个系统中，上下层之间则通过接口进行通信，用“服务访问点”（SAP）来定义接口。SAP 就是一个层次系统的上下层之间进行通信的接口，N 层的 SAP 就是 $N+1$ 层可以访问 N

层服务的地方。

为了对 OSI 参考模型中的多个高层实体提供支持，在局域网参考模型中的 LLC 子层的顶部有多个 LLC 服务访问点（LSAP），为 OSI 高层提供接口端。媒体访问控制服务访问点（MSAP）向 LLC 实体提供单个接口端。物理服务访问点（PSAP）向 MAC 实体提供单个接口端。在 OSI 参考模型的网络层的顶部有多个网间服务访问点（NSAP），为传输层提供接口端。这样的局域网体系结构不仅使得 IEEE 802 标准更具有可扩充性，有利于其将来接纳新的介质访问控制方法和新的局域网技术，同时也不会使局域网技术的发展或变革影响到网络层。

4.1.4 IEEE 802 标准

在 20 世纪 80 年代初期，美国电气和电子工程师学会 IEEE 802 委员会首先制定出局域网的体系结构，即著名的 IEEE 802 参考模型。许多 802 标准现已成为 ISO 国际标准。

局域网的体系结构与广域网的有相当大的区别。由于局域网只是一个计算机通信网，而且局域网不存在路由选择问题，因此它不需要网络层，而只有最低的两个层次。然而局域网的种类繁多，其媒体接入控制的方法也各不相同，远远不像广域网那样简单。为了使局域网中的数据链路层不致过于复杂，就应当将局域网的数据链路层划分为两个子层，即媒体接入控制或媒体访问控制 MAC（Medium Access Control）子层和逻辑链路控制 LLC（Logical Link Control）子层，而网络的服务访问点 SAP 则在 LLC 层与高层的交界面，如图 4-2 所示。局域网的参考模型就只相当于 OSI 的最低的两层。

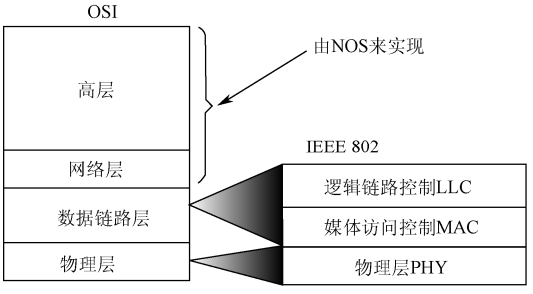


图 4-2　IEEE 802 标准（LAN 参考模型）

IEEE 802 委员会现有以下 13 个分委员会，分别负责以下方面的标准的研究与制定。

（1）802.1——概述、体系结构和网络互联，以及网络管理和性能测量。

（2）802.2——逻辑链路控制。这是高层协议与任何一种局域网 MAC 子层的接口。

（3）802.3——CSMA/CD。定义 CSMA/CD 总线网的 MAC 子层和物理层的规约。

（4）802.4——令牌总线网。定义令牌传递总线网的 MAC 子层和物理层的规约。

（5）802.5——令牌环型网。定义令牌传递环型网的 MAC 子层和物理层的规约。

（6）802.6——城域网 MAN。定义城域网的 MAC 子层和物理层的规约。

（7）802.7——宽带技术。

（8）802.8——光纤技术。

（9）802.9——综合语音数据局域网。

（10）802.10——可互操作的局域网的安全。

（11）802.11——无线局域网。

（12）802.12——优先级高速局域网（100Mbps）。

（13）802.13——电缆电视（Cable-TV）。

这里要指出，城域网 MAN（Metropolitan Area Network）的地理范围比局域网的大，可跨越几个街区甚至整个城市。城域网具有中速到高速的通信信道，其差错率和时延可以略高于局域网的指标。一个城域网可以为一个或几个单位所拥有，但也可以是一种公用设施，用来将多个局域网进行互联。城域网与局域网使用相同的体系结构，有时也常常并入局域网的范围。

4.2　介质访问控制方法

局域网中的计算机都连接在一个公共信道上，即所有节点共享介质。这个特点使网络节点如何有序访问共享介质或者说如何为每个节点分配信道，成为了影响局域网性能的重要因素。介质访问控制（MAC）方法是在局域网中对数据传输介质进行访问管理的方法。介质访问控制方法的主要内容有两个方面：一是要确定网络上每一个节点能够将信息发送到介质上去的特定时刻；二是要解决如何对共享介质访问和利用加以控制。

传统局域网采用共享介质方式的载波监听多路访问/冲突检测（CSMA/CD）、标记环传递或 FDDI 等方法，如图 4-3 所示。但随着 LAN 应用的扩展，这种共享介质方式对任何端口上的数据帧都不加区别地进行传送时，经常会引起网络冲突甚至阻塞，所以采用网桥、交换机等方法将网络分段，减少甚至取消网络冲突是目前经常采用的方法。

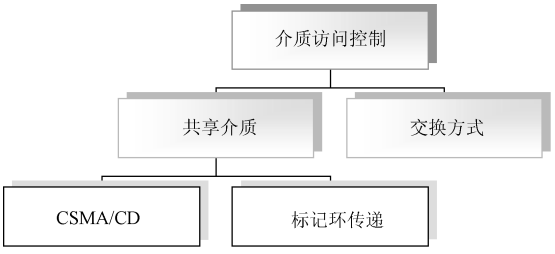


图 4-3　介质访问控制方法

4.2.1　信道分配问题

通常可将信道分配方法划分为两类：静态分配方法和动态分配方法。

1．静态分配方法

所谓静态分配方法，也是传统的分配方法，它采用频分多路复用或时分多路复用的办

法将单个信道划分后静态地分配给多个用户。当用户站数较多或使用信道的站数在不断变化或者通信量的变化具有突发性时，静态频分多路复用方法的性能较差，因此，传统的静态分配方法，不完全适合计算机网络。

2．动态分配方法

所谓动态分配方法，就是动态地为每个用户站点分配信道使用权。动态分配方法通常有 3 种：轮转、预约和争用。

① 轮转：使每个用户站点轮流获得发送的机会，这种技术称为轮转。它适合于交互式终端对主机的通信。

② 预约：预约是指将传输介质上的时间分隔成时间片，网上用户站点若要发送，必须事先预约能占用的时间片。这种技术适用于数据流的通信。

③ 争用：若所有用户站点都能争用介质，这种技术称为争用。它实现起来简单，对轻负载或中等负载的系统比较有效，适合于突发式通信。争用方法属于随机访问技术，而轮转和预约的方法则属于控制访问技术。

4.2.2 介质访问控制方法

以太网的介质访问控制方法——带冲突检测的载波监听多路访问（CSMA/CD），冲突检测/载波监听（CSMA/CD）是以太网中采用的介质访问控制方法，它的控制规则是各用户之间采用竞争方法抢占传输介质以取得发送信息的权利。CSMA/CD 的工作原理可以概述为“先听后发，边听边发，冲突停发，随机重发”，它不仅体现在以太网中数据的发送过程中，同时也体现在数据的接收过程中。

CS——载波监听：每个节点监视网络状况，确定是否有其他节点在发送数据；

MA——多路访问：网络中的多个节点可能试图同时发送数据；

CD——冲突检测：每个节点通过比较自己发送的信息是否受损来检测信号的冲突。

冲突检测/载波监听（CSMA/CD）介质访问控制的工作过程如下：

① 发送信息的站点首先“监听”信道，看是否有信号在传输，如果发现信道正忙，就继续监听；

② 如信道空闲，就可以立即发送数据；注意此时可能有两个或更多个站点同时都在监听并发现信道空闲，而在信道空闲后有可能同时发送数据；

③ 发送信息的站点在发送过程中同时监听信道，检测是否有冲突发生。发生冲突的结果是双方的数据都受损。发送方通过接收信道上的数据并与发送的数据进行比较，就可以判断是否发生了冲突。

④ 当发送方检测到冲突后，就立即停止数据的传输，并向信道上发长度为 4 字节的“干扰”信号，以确保其他站点也发现该冲突。然后，等待一段时间再尝试发送。

目前，常见的局域网中，一般都采用 CSMA/CD 访问控制方法的逻辑总线型网络，用户只要使用 Ethernet 网卡，就具备此种功能。

4.3　局域网的组成

组成一个局域网有三大要素：网络结构、网络硬件系统及网络软件系统。在三大要素中，通常首先要考虑选择网络软件系统，根据网络软件系统选定所支持的网络结构，并由此确定网络硬件设备。在本节中首先学习局域网的硬件及软件系统。

4.3.1 局域网硬件系统

通常组建局域网需要的网络硬件主要是服务器、网络工作站、网络适配器（网卡）、交换机及传输介质等。

1．服务器

服务器（Server）是以集中方式管理局域网中的共享资源，为网络工作站提供服务的高性能、高配置计算机。常见的有文件、打印和异步通信三种服务器。

文件服务器常采用高档微型计算机，它给用户提供了操作系统、文件系统的各种功能，如生成文件、删除文件等。

打印服务器是安装了打印服务程序的文件服务器或专用微型计算机。用户共享的打印机连在打印服务器上，在网络环境下，网上用户可将打印数据送到打印服务器的打印队列中，将数据从打印机输出。

异步通信服务器是装有相应通信软件的文件服务器或专用微型计算机，利用调制解调器（MODEM）通过电话线或专用的通信线路连接远程工作站。在网络环境下，网上用户可通过异步通信服务器与远程工作站通信。

2．网络工作站

网络工作站（WorkStation），是网络用户最终的操作平台，用户通过它来访问网络的共享资源。在局域网中，工作站一般采用微型计算机，除了访问网络资源外，本身具有一定的处理能力，可独立工作。根据应用的需要，工作站也可以是无盘的，称为无盘工作站。

3．网络适配器

网络适配器又称网络接口卡（Network Interface Card，NIC），简称网卡，是计算机网络中最基本和最重要的连接设备之一，如图 4-4 所示。它在网络中的主要作用是：一方面负责接收网络中传输的数据包，解包后将数据通过总线传输给本地计算机，另一方面将本地计算机的数据经过打包后传送至网络中传输。

图 4-4　网络适配器

它通常是一块独立的插件板，插在计算机主板的扩展槽中，通过网卡上的接口与网络

的电缆系统连接，从而将服务器、工作站连接到传输介质上并进行电信号的匹配，实现数据传输。

网卡有多种类型，其中根据网络使用的传输介质，可分为有线网卡和无线网卡；按照总线接口类型一般可分为 PCI 接口网卡、PCI-E 接口网卡和 USB 接口网卡等；按照网络接口类型可分为 AUI 粗同轴电缆接口网卡、BNC 细同轴电缆接口网卡、RJ-45 双绞线接口网卡和 F/O 光纤接口网卡等；根据数据传输速率不同可分为 100M 网卡、100/1000M 自适应网卡及万兆网卡。

选择网卡时应从计算机总线的类型、传输介质的类型、组网的拓扑结构、节点之间的距离及网络段的最大长度等几个方面来考虑。目前常用的网卡是采用 RJ-45 接口的 100/1000M 自适应网卡。

4．交换机

图 4-5　24 口的网络交换机

交换机（Switch）是一种用于电信号转发的网络设备。它可以为接入交换机的任意两个网络节点提供独享的电信号通路。最常见的交换机是以太网交换机。其他常见的还有电话语音交换机、光纤交换机等。交换机能把用户线路、电信电路和（或）其他要互联的功能单元根据单个用户的请求连接起来。如图 4-5 所示为 24 口的网络交换机。

5．传输介质

传输介质也称为通信介质或媒体，在网络中充当数据传输的通道。传输介质决定了局域网的数据传输速率、网络段的最大长度、传输的可靠性及网卡的复杂性。

局域网的传输介质主要是双绞线、同轴电缆和光纤。

早期的局域网中使用最多的是同轴电缆。伴随着技术的发展，双绞线和光纤的应用越来越广泛，目前在局部范围内的中、高速局域网中使用双绞线，在较远范围内的局域网中使用光纤已很普遍。

4.3.2　局域网软件系统

如果计算机只有硬件而没有软件将既不能启动也无法运行，更无法完成任何工作，同样，没有网络操作系统和网络协议的网络，也将无法实现计算机之间彼此的通信，网络设备也只能是一堆摆设。而计算机在网络中的地位，主要是由网络操作系统来决定的。

组建局域网的基础是网络硬件，网络的使用和维护要依赖于网络软件。在局域网上使用的网络软件主要是网络操作系统、网络数据库管理系统和网络应用软件。

1．局域网操作系统

网络操作系统（Network Operating System，NOS）是用来管理网络上的各种计算机，使用户能方便有效地共享网络资源，为网络用户提供所需的各种服务的软件和有关规程的

集合。网络操作系统是网络环境下用户与网络资源之间的接口，用以实现对网络的管理和控制。

网络操作系统可以用来监视网络的运行状况、管理网络的共享资源、保证资源的安全、优化网络的性能和排除网络的故障，以此确保网络能够高效可靠地工作并为用户提供各种网络服务。与单机操作系统相比，网络操作系统偏重于将与网络活动相关的特性加以优化，即通过网络来管理诸如共享数据文件、软件应用和外部设备之类的资源。而单机操作系统则偏重于优化用户与系统的接口以及在其上面运行程序的应用。网络操作系统的水平决定着整个网络的水平，及能否使所有网络用户都能方便、有效地利用计算机网络的功能和资源。

局域网操作系统主要由服务器操作系统、网络服务软件、工作站软件及网络环境软件 4 部分组成。

目前，常用的局域网操作系统有：Microsoft 公司的 Windows 系列（如 Windows Server 2008 等），Linux 以及功能强大的 UNIX 系统。它们在技术、性能、功能方面各有所长，支持多种工作环境，支持多种网络协议，能够满足不同用户的需要，为局域网的广泛应用奠定了良好的基础。

在选择网络操作系统时，应从它对当前所组建网络的适应性和总体性能方面考虑，包括系统的效率、可靠性、安全性、可维护性、可扩展性、管理的简单方便性及应用前景等内容。

（1）Windows Server2008

Windows Server 2008 是美国微软公司在 2008 年推出的网络操作系统。它几乎成为中、小型企业局域网的标准操作系统，一是因为它继承了 Windows 家族统一的界面，使用户学习、使用起来更加容易。其次是它的功能也的确比较强大，基本上能满足所有中、小型企业的各项网络需求。

Windows Server 2008 的主要特点是：硬件的独立性较强，网络操作系统能在不同的硬件平台上运行；具有强大的管理特性，如系统备份、容错性能控制等；Windows Server 2008 是一个高性能的客户/服务器应用平台，支持多种网络协议，具有目录服务功能；通过域（domain）的概念来对用户资源进行控制，并提供简单的方法来控制用户对网络的访问；具有良好的用户界面，支持多窗口操作；具有自动再连接特性，即当服务器从故障中恢复正常时，能重新建立与工作站的通信；虚拟化是 Windows Server 2008 的一个重大创新功能，利用虚拟化功能可创建多台虚拟服务器，最大限度地发挥 Windows Server 2008 的作用。但 Windows Server 2008 对硬件的要求较高，所占的内存空间较大。

（2）UNIX

UNIX 是 20 世纪 60 年代由美国贝尔实验室开发的一种多用户、多任务的网络操作系统，被广泛应用于网络服务器、Web 服务器、数据库服务器等高端领域。

UNIX 系统最突出的一个特点是可靠性高。UNIX 在用户权限、文件和目录权限、内存管理方面都有严格的规定，使系统的安全性、稳定性得到了充分的保障。另外在网络信息的保密性、数据的安全备份等方面也都提供了很好的保护措施。另一个主要特点是 UNIX 具有很强的联网功能，作为 Internet 技术基础的 TCP/IP 协议就是在 UNIX 上开发出来的，而且成为 UNIX 不可分割的组成部分，正是因为 UNIX 和 TCP/IP 的完美结合，促进了

UNIX、TCP/IP 以及 Internet 的推广和普及。目前 UNIX 一直是 Internet 上各种服务器的首选操作系统。

UNIX 的缺点是系统过于庞大，命令复杂，一般用户很难掌握。同时，UNIX 的内核技术公开后，很多公司根据自身的特点和发展推出了自己的 UNIX 版本，但这些版本之间互不兼容，这也成为 UNIX 系统推广应用的障碍。

（3）Linux

Linux 是一个“类 UNIX”的操作系统，1991 年由芬兰赫尔辛基大学的一名学生开发。Linux 是自由软件，也称源代码开放软件，用户可以免费获得并使用 Linux 系统，并可以继续开发并重新发布。

Linux 支持几乎所有的硬件平台，包括 Intel 及 Apple 等系统，并广泛支持各种周边设备。Linux 采用了包括对读和写进行权限控制及核心授权等许多安全技术措施，为网络用户提供了必要的安全保障。另外，Linux 也为用户提供了完善且强大的网络功能。

Linux 系统的主要缺点是：版本繁多，且不同版本之间存在大量的不兼容之处，同时相对于 Windows 系统来说，Linux 易用性较差。

2．网络数据库管理系统

网络数据库管理系统是一种可以将网上的各种形式的数据组织起来，科学、高效地进行存储、处理、传输和使用的系统软件。可把它看做网上的编程工具，如 My SQL、SQL Server、Oracle、Informix 等。

3．网络应用软件

软件开发者根据网络用户的需要，利用开发工具开发的能够为网络用户提供各种服务的软件。网络应用软件为用户提供访问网络的手段，用于发布或获取网络上的共享资源，例如，常见的面向企业局域网终端使用者的网络沟通工具 RTX 软件、Internet 信息服务软件等。

4.4　局域网的工作模式

不同的网络模式，其工作特点和所提供的服务是不同的，因此用户应当根据所运行的应用程序的需要，选择合适的网络模式。

局域网在发展进程中的几种网络模式分别有以下几种系统结构。

（1）集中式处理的主机－终端机系统结构。

（2）对等网络系统结构。

（3）客户机–服务器系统结构

（4）浏览器–服务器系统结构。

在这几种结构中，主机–终端机系统结构主要应用于银行等具有特殊要求的计算机网络系统，在局域网中不多见。

4.4.1 对等结构网络

对等网络是指网络上每个计算机的地位都是平等的或者是对等的。没有特定的计算机作为服务器。在 Windows 系列操作系统中，对等网络又称为工作组网络（Workgroup）。

1．对等网

对等网也可以说成是不要服务器的局域网，它是一个分布式网络系统。在对等网中资源和管理是分散在网络中的各个工作站上的，网络中的每一台计算机之间不是“服务器-工作站”的关系，也不是“客户机-服务器”的关系，在对等网上各台计算机都有相同的功能，没有主从之分，网上的任意节点计算机既可以作为网络服务器为其他计算机提供资源，也可以作为工作站，分享其他计算机上的资源。它们之间是对等的，充分利用了点到点通信的功能。

在对等网中，各工作站除了共享文件之外，还可以共享打印机。对等网上的打印机可被网络上的任意节点使用，如同使用本地打印机一样方便。因为对等网不需要专门的服务器来做网络支持，也不需要其他组件来提高网络的性能。

2．对等网的规划

对等网络的规划一般比较简单，通常采用如图 4-6 所示的星型结构或如图 4-7 所示的总线型结构。

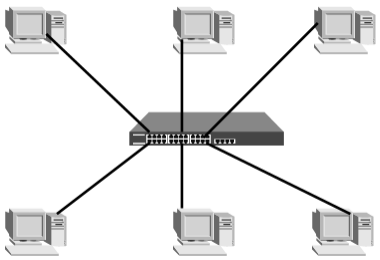


图 4-6　星型结构对等网

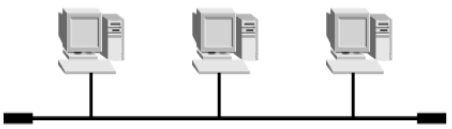


图 4-7　总线型结构对等网

现多采用星型拓扑结构。星型结构对等网用户要选购的硬件包括：① 交换机；② 每台上网的计算机配置一块带有 RJ-45 接口的网卡；③ 每台上网的计算机配置一根末端装有 RJ-45 接头的双绞线，双绞线的长度视计算机与交换机的距离而定，一般在 100m 以内。

3．对等网的适用场合

对等网适用于小型办公室、实验室和家庭等小规模网络，通常对网络计算机工作站的要求是最好不超过 10 台计算机，超过 10 台计算机以后，对等网的维护会变得十分困难。所以当用户的计算机数量不多时，并以资源共享为主要目的时，建议采用这种网络结构。

4．对等网的特点

（1）主机地位相等

在对等网络中的每一个计算机，当要使用网络中的某种资源时它就是客户机，当它为网络的其他用户提供某种资源时，就成为服务器，所以在对等网络中的计算机既可作为服务器也可作为客户机。实际上，在网络上所有的打印机、光驱、硬盘、调制解调器等诸多设备都能进行共享。

（2）管理方便

对等网络中每台计算机都有绝对的自主权，自行管理自己的资源和账户，用户自行决定资源是否共享，其管理方式是分散的。但也因其安全性较差，复杂的网络管理功能（如安全的远程访问等）无法实现。

（3）成本低廉

对等网不需要专用服务器，不需要功能强大的交换设备，系统配置简单，维护费用低。

在用户对网络功能和服务要求不高的小型局域网建设中，对等网络可以满足用户的需要，如办公室、家庭和游戏厅等小规模网络。

4.4.2 客户机/服务器模式

客户机/服务器网络（C/S）是以服务器为中心的网络模型，也称为主-从结构网络。在 20 世纪 90 年代相当流行，这种网络模型价格低廉，资源共享灵活简单，有良好的可扩充性。

1．客户机/服务器网络

客户机/服务器网络结构是在专用服务器结构的基础上发展起来的。随着局域网的不断扩大和改进，在局域网的服务器中共享文件、共享设备的服务仅仅是典型应用中很小的一部分。网络技术的发展使得文件服务器也可以完成一部分应用处理工作。每当用户需要一个服务时，由工作站发出请求，然后由服务器执行相应的服务，并将服务的结果送回工作站。这时，工作站已不再运行完整的程序，其身份也自然从“工作站”变为“客户机”。局域网中需要处理的工作任务分配给客户机端和服务器端共同来完成。

2．客户机/服务器网络的规划

客户机/服务器网络的规划，通常采用如图 4-8 所示的星型拓扑结构，使用专用的服务器为网络用户提供服务。服务器有文件服务器、应用服务器等。服务器是局域网中的核心设备，一般由高档的计算机或专用服务器来担任。它有大容量的内存和硬盘，以及高速的 CPU，服务器上安装有网络操作系统，用户可以共享服务器上的网络资源。

星型结构客户机/服务器网络用户要选购的硬件包括：① 服务器；② 交换机；③ 每台上网的计算机配置一块带有 RJ-45 接口的网卡；④ 每台上网的计算机配置一根末端装有 RJ-45 接头的双绞线，双绞线的长度视计算机与交换机的距离而定，一般在 100m 以内。

3．客户机/服务器网络的适用场合

C/S 结构具有广泛的适用性，因此被应用于各种要求安全性能较高、便于管理、具有各

种计算机档次的中小型单位，如公司的办公网络、工商企业网、校园网和园区网等。

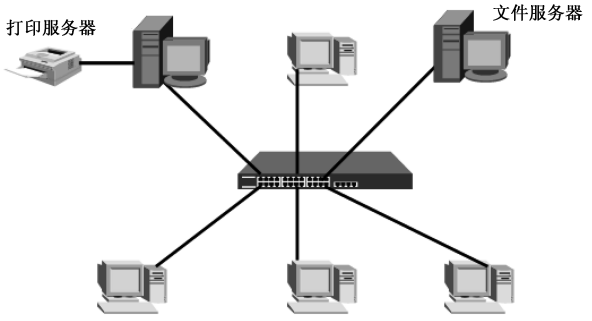


图 4-8　客户机/服务器网络结构

4．客户机/服务器模式（C/S）的特点

（1）分工明确

在客户机/服务器模型中，网络中计算机分工明确。服务器就是负责网络资源的管理和提供网络服务的，客户机向服务器请求服务和访问共享资源。明确分工便于将重要的数据集中，使访问变得更加方便和安全，而且可以提供强大的网络服务。这是对等网无法做到的。

（2）集中式管理

这种网络模型中，服务器承担集中式网络的管理工作。从用户身份的验证到资源访问控制都是在服务器上进行的，网络管理更加方便和专业。客户机不需要进行网络管理工作，只关注网络的使用。

（3）可扩充性好

客户机/服务器模型的可扩充性优于对等网。在对等网络中，添加一台主机，由于对资源控制的需要，可能需要在网络中每台主机上都进行一定的配置；在客户机/服务器模型中，当需要增加主机时，不需要重新设计，直接增加计算机即可。

4.4.3　浏览器/服务器模式

B/S 结构（Browser/Server 结构），即浏览器/服务器结构。它是随着 Internet 技术的兴起，对 C/S 结构的一种变化或者改进的结构。在这种结构下，用户工作界面通过 WWW 浏览器来实现，极少部分事务逻辑在前端（Browser）实现，但是主要事务逻辑在服务器端（Server）实现，形成所谓三层（3-tier）结构。这样就大大简化了客户端计算机载荷，减轻了系统维护与升级的成本和工作量，降低了用户的总体成本。

随着 Internet 和 WWW 的流行，以往的主机-终端和 C/S 都无法满足当前的全球网络开放、互联、信息随处可见和信息共享的新要求，于是就出现了 B/S 型模式，即浏览器/服务器结构。B/S 模式最大特点是用户可以通过 WWW 浏览器去访问 Internet 上的文本、数据、图像、动画、视频点播和声音信息，这些信息都是由许多的 Web 服务器产生的，而每一个

Web 服务器又可以通过各种方式与数据库服务器连接，大量的数据实际存放在数据库服务器中。客户端除了 WWW 浏览器，一般无须任何用户程序，只需从 Web 服务器上下载程序到本地来执行，在下载过程中若遇到与数据库有关的指令，由 Web 服务器交给数据库服务器来解释执行，并返回给 Web 服务器，Web 服务器又返回给用户。

在这种结构中，将许许多多的网络连接到一块，形成一个巨大的网络，即全球网络。而各个企业可以在此结构的基础上建立自己的 Intranet。

以目前的技术看，局域网建立 B/S 结构的网络应用，并通过 Internet/Intranet 模式下数据库应用，相对易于把握，成本也是较低的。它是一次性到位的开发，能实现不同的人员，从不同的地点，以不同的接入方式（如 LAN、WAN、Internet/Intranet 等）访问和操作共同的数据库；它能有效地保护数据平台和管理访问权限，服务器数据库也很安全。特别是在 Java 这样的跨平台语言出现之后，B/S 架构管理软件更是方便、速度快、效果优。

1．浏览器/服务器模式（B/S）的优点

（1）具有分布性特点，可以随时随地进行查询、浏览等业务处理。

（2）业务扩展简单方便，通过增加网页即可增加服务器功能。

（3）维护简单方便，只需要改变网页，即可实现所有用户的同步更新。

（4）开发简单，共享性强。

2．浏览器/服务器模式（B/S）的缺点

（1）个性化特点明显降低，无法实现具有个性化的功能要求。B/S 模式完全基于服务器，脱离服务器就无法正常运行。

（2）操作是以鼠标为最基本的操作方式，无法满足快速操作的要求。B/S 模式中用户必须使用辅助的插件，才可以用键盘进行快速操作。

（3）页面动态刷新，响应速度明显降低。B/S 模式对服务器要求过高、数据传输速度慢。

（4）功能弱化，难以实现传统模式下的特殊功能要求。例如通过浏览器进行大量的数据输入或进行报表的应答、专用性打印输出都比较困难和不便。

（5）面临的安全威胁较大。B/S 模式中的用户都是不可知的，需要加强防护。

4.5 典型局域网

局域网作为日常生活中最常见的计算机网络，并不是千篇一律地采用同一个模式来构建的，对于不同的网络规模、网络功能，在实现方法上也有所不同。目前，常见的局域网大致分为以下几种类型。

4.5.1 传统以太网

以太网在已有的各种局域网标准中，是应用最为广泛、最为成熟的一种局域网技术，由美国的施乐公司于 1975 年研制成功。采用 CSMA/CD（冲突检测/载波监听）介质访问控

制方法，使用的典型拓扑结构是总线型，传输速率理论值为10Mbps，实际的传输速率为2M～3Mbps，不适用于大型或忙碌的网络。常见的以太网有 4 种类型：10Base5、10Base2、10Base-T 和 10Base-F，其传输介质分别为粗缆、细缆、双绞线和光纤。

4.5.2 快速以太网

快速以太网与以太网非常类似，执行的是以太网的扩展标准，保留着传统以太网的所有特征：相同的数据格式、介质访问控制方法与组网方法，将数据发送时间由 100ns 降低为 10ns，传输速率可达 100Mbps。快速以太网主要有两种类型：100Base-T 和 100Base-VG，这两种快速以太网的主要区别在于介质访问控制方法不同，100Base-T 仍采用了 CSMA/CD 介质访问控制方法，而 100Base-VG 则采用了新的介质访问方法——请求优先。快速以太网可以使用的传输介质为光纤和五类非屏蔽双绞线。

100Base-T 以太网主要分为 100Base-TX 和 100Base-FX 两种技术，其中 100Base-TX 标准使用两对 5 类非屏蔽双绞线作为传输介质，一对用于发送数据，另一对用于接收数据，每段最大长度为 100m。100Base-FX 采用两对光纤作为传输介质，适用于高速主干网、有电磁干扰的环境和要求通信保密性好、传输距离远等应用场所，但 100Base-FX 标准并没有被广泛应用。

4.5.3 高速以太网

千兆以太网是目前速率最快的网络，它与以太网、快速以太网相似，采用同样的 CSMA/CD 介质访问控制方法，同样的帧格式，传输速率可达 1Gbps，并向下兼容现有的 10M 以太网和 100M 快速以太网，能够将 10Mbps、100Mbps 和 1000Mbps 三种不同的传输速率完美地组织成一个网络，是现有以太网最自然的升级途径。千兆以太网（万兆以太网）可以使用的传输介质为光纤和 5 类非屏蔽双绞线。

4.5.4 ATM 网

ATM 是高速分组交换技术，其基本数据传输单元是信元。在 ATM 交换方式中，文本、语音、视频等所有数据被分解成长度固定的信元，信元由一个 5 字节的元头和一个 48 字节的用户数据组成，长度为 53 字节。ATM 数据传输就是在高频通道中建立虚拟通道和虚拟路径，并利用高速交换机将被分割为固定长度的信元执行非同步的信元交换，其速率可达 155Mbps。ATM 网具有以下一些优点：

（1）ATM 网的网络用户可以独享全部频宽，即使网络中增加计算机的数量，传输速率也不会降低；

（2）由于 ATM 数据被分成等长的信元，能够比传统的数据包交换更容易达到较高的传输速率；

（3）能够同时满足数据及语音、影像等多媒体数据的传输需求；

（4）可以同时应用于广域网和局域网中，无须选择路由，可以大大提高广域网的传输

速率。它必须使用光纤作为传输介质，主要应用于主干网上。

4.5.5 FDDI 网

光纤分布数据接口（FDDI）标准是由美国国家标准协会建立的一套标准，它使用基本令牌的环型体系结构，以光纤为传输介质，传输速率可达 100Mbps，主要用于高速网络主干，能够满足高频宽信息的传输需求。它具有以下一些特点：

（1）传输介质采用光纤，抗干扰性和保密性好；

（2）为备份和容错起见，一般采用双环结构，可靠性高；环的最大长度为 100km，适用场合较广；

（3）具有规模大，差错率低，传输速率高的特点，能够满足宽带应用的要求；

（4）造价太高，主要应用于大型网络的主干网中。

4.5.6 无线局域网

无线局域网 WLAN（Wireless Local Area Network）是计算机网络与无线通信技术相结合的产物，移动通信技术的飞速发展也为无线接入提供了基础。WLAN 可提供移动接入的功能，一般采用红外线（IR）和无线电射频（RF）技术，而 RF 技术使用得更多一点，因为其覆盖范围更广、传输速率更高。许多无线局域网使用 2.4GHz 波段，该波段在全世界范围内是可以自由使用的。

1．无线局域网的标准

目前无线局域网仍处于众多标准共存时期，不同的标准有不同的应用。主要的无线局域网标准有 IEEE 802.11 协议簇、蓝牙协议、HomeRF 等。

IEEE 802.11 系列标准中主要包括 IEEE 802.11、IEEE 802.11a、IEEE 802.11b、IEEE 802.11g 和 IEEE 802.11n 等多个标准。IEEE 802.11 是最早制定的一个无线局域网标准，数据传输速率最高只能达到 2Mbps。在这之后，IEEE 802.11 标准体系与技术发展非常迅速，1999 年出现了 IEEE 802.11a，它使用 5GHz 频段，数据传输速率达到 54Mbps；IEEE 802.11b 技术适合企业用户，工作在 2.4GHz 频段，最高传输速率可达到 11Mbps，能根据传输距离自动调整到 5.5Mbps、2Mbps、1Mbps 等速率，最大传输距离为 150m 左右，通过增加发射功率可以达到 300m 左右，但 IEEE 802.11a 与 IEEE 802.11b 标准的工作频段不一样，导致相互不兼容。

2003 年 IEEE 推出了新版 IEEE 802.11g 认证标准，IEEE 802.11g 标准是为 IEEE 802.11b 提速而设计的，也工作在 2.4GHz 频段，数据传输速率达到 54Mbps，并且与 IEEE 802.11b 标准完全兼容。

IEEE 802.11n 是 2009 年发布的一个新标准，最大的特点是速率提升，理论速率最高可达 600Mbps，802.11n 为双频工作模式，可工作在 2.4GHz 和 5GHz 两个频段，向下兼容 802.11a/b/g 标准。另外，采用的多项新技术使无线局域网的传输距离大大增加，覆盖范围可以达到几千米。IEEE 802.11n 标准目前已发展成无线局域网的主要标准。

红外线技术 IR 是指波长为 850～950nm 的红外线在室内传输数据，速率为 1M～2Mbps。红外线技术的最大优点是不受无线电的干扰，且红外线的使用不受国家无线管理委员会的限制。一般家电遥控器大多数都是采用红外线技术。但红外线对非透明物体的穿过性极差，因此传输距离受限制，大多情况下是在单个房间内使用。

蓝牙（Bluetooth）协议是低带宽、短距离、低功耗的数据传输技术，用于手机、笔记本电脑等设备中。蓝牙（Bluetooth）协议和 IEEE 802.11b 可以同时工作。

HomeRF 是由 HomeRF 工作组开发的，适合家庭区域范围内，在计算机和用户电子设备之间实现语音和数据传输的无线通信技术。但是，该标准与 IEEE802.11b 不兼容，并占据了与 IEEE 802.11b 和蓝牙相同的 2.4GHz 频率段，所以在应用范围上会有很大的局限性，更多的是在家庭网络中使用。

2．无线局域网的用途

无线局域网节点之间的连接不需要电缆，在组建、使用和扩充时就十分方便灵活。其主要用途有以下 4 个方面。

（1）扩充有线局域网

通过无线访问点可以把无线局域网联入有线局域网，特别是需要把局域网的范围扩大到一些电缆布线不便的场所时，这种连接方式尤为必要。

（2）连接建筑物之间局域网

被连接的局域网可以是有线的，也可以是无线的。当两个建筑物被河流、高速公路等隔开的情况下，使用无线网络连接两个建筑物之间的局域网是一种明智的选择。

（3）实现漫游访问

漫游访问是指为带无线网卡的笔记本电脑等移动设备提供到有线局域网的连接。移动节点可能通过不同的访问点接入有线网。

（4）构建临时网

一个临时需要的对等网络使用无线网络来实现显然比较方便，如学术会议论文交流、交易会产品信息互通。把参加者的计算机连接到一个临时的网络上，会议结束后网络自然就撤除了。

3．无线局域网传输技术

无线局域网的传输技术常用的有两种：红外线辐射传输技术和扩展频谱技术。无线局域网中最具发展前景的、目前使用最广泛的是扩展频谱技术。

（1）基于红外线的无线局域网

红外线辐射技术的特点是：红外线的波长比光谱颜色波的波长要长，但比无线电波的波长短得多，大多数有光的地方，肉眼是看不到红外线的。红外线不能穿透诸如墙壁等不透明物体，往往通信距离较短，但可以保护数据安全，因为在障碍物之外的人不可能直接截取到红外线信号，所以比较适用于近距离点对点传输的环境。但是，由于自身覆盖范围的限制，红外线并不是很适用于移动连接。

常见的基于红外线的无线局域网有两种，一种是漫射红外线无线局域网，另一种是点对点红外线无线局域网。

① 漫射红外线无线局域网。一直以来，人们都在使用漫射红外线设备——电视遥控器，它让用户在一定距离操作电视机而无须连线。当用户按下遥控器的一个按钮时，相应的编码调制红外线信号传输到电视机，电视机接收到信号，执行相应的功能。基于红外线的局域网的道理也是如此，主要区别是后者以较高的功率利用红外线并使用通信协议来传输数据。在房间里，通常天花板、四周的墙壁都会成为反射点，所以在这种方式下，信号的传输依赖于天花板和墙壁，如图 4-9 所示。所以漫射红外线无线局域网不能在室外操作。

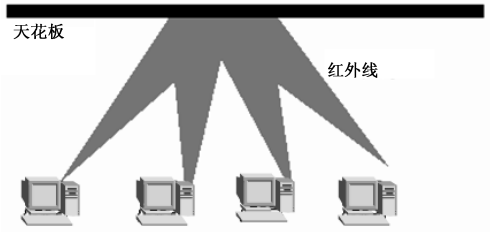


图 4-9　基于漫射红外线的无线局域网

② 点对点红外线无线局域网。在点对点红外线无线局域网中，包含一对收发器，一个用于发送，另一个用于接收。目前这种点对点红外线无线局域网技术运用得并不是很多。

（2）扩展频谱技术

扩频就是把要传送的窄带信号扩展到比原频带宽得多的频带上，使其功率频谱密度大大降低，将信号淹没在噪声中。在接收端，用相关接收的方法将宽带信号恢复成窄带信号。扩展频谱技术目前在无线局域网中应用较广。

扩展频谱具有以下的特点。

① 很强的抗干扰能力。由于将信号扩展到很宽的频带上，在接收端对扩频信号进行相关处理即带宽压缩，恢复成窄带信号。对干扰信号而言，由于与扩频用的伪随机码不相关，则被扩展到很宽的频带上，使之进入信号通频带内的干扰功率大大降低，因此具有很强的抗干扰能力。其抗干扰能力与其频带的扩展倍数成正比，频谱扩展得越宽，抗干扰的能力越强。

② 安全保密。由于扩频系统将传送的信号扩展到很宽的频带上去，其功率密度随频谱的扩宽而降低，甚至可以将通信信号淹没在噪声中。因此，其保密性很强，要截获、窃听或侦察这样的信号是非常困难的。

③ 抗多径干扰。在移动通信、室内通信等通信环境下，多径干扰是非常严重的，系统必须具有很强的抗干扰的能力，才能保证通信的畅通。扩展频谱技术具有很强的抗多径干扰能力，它是利用扩频所用的扩频码的相关特性来达到抗多径干扰，甚至可以利用多径能量来提高系统的性能。

④ 可进行多址通信。扩展频谱通信本身就是一种多址通信方式，称为扩频多址，用不同的扩频码组成不同的网。虽然扩展频谱系统占用了很宽的频带，但由于各网在同一时刻共用同一频段，其频段利用率非常高。

在现有的无线局域网中，大都采用扩频技术，以此来提高系统性能，满足对系统提出的各种要求。采用比较多的扩频方式是直接序列和跳频。

直接序列扩展频谱技术是目前应用较广的一种扩频方式。直接序列扩频系统是将要发

送的信息用伪随机码（PN 码）扩展到一个很宽的频带上去，在接收端，用与发射端扩展用的相同的伪随机码对接收到的扩频信号进行相关处理，恢复发送的信息。对干扰信号而言，由于与伪随机码不相关，在接收端被扩展，使落入信号通频带内的干扰信号功率大大降低，从而达到了抗干扰的目的，如图 4-10 所示。

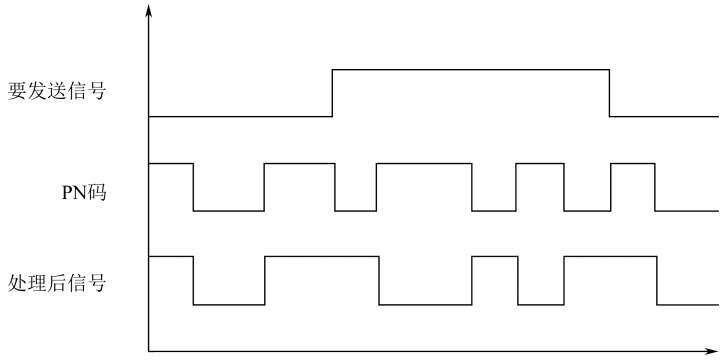


图 4-10　直接序列扩展频谱技术示意图

跳频扩展频谱技术，它发送数字信号，然后用载波信号调制，载波信号在一个很宽的频带上从一个频率跳变到另一个频率。两种扩频方式相比较，如果网络所需的带宽为 2Mbps 或更小，跳频是无线局域网中性价比最可取的，而直接序列则具有更大的潜在数据速率，对于要求更高带宽的应用来讲是最佳选择，如图 4-11 所示。

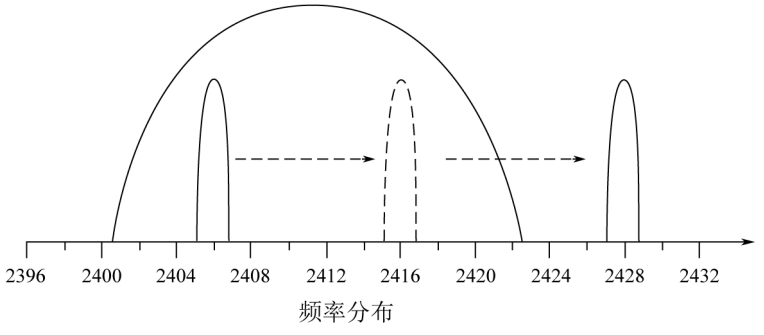


图 4-11　跳频扩展频谱技术示意图

扩展频谱技术备受重视，它使无线局域网的抗干扰能力、多址功能、安全保密性能、抗多径干扰性能大大提高，为无线局域网的推广和应用奠定了基础。

4．无线局域网设备

一般来说，组建无线局域网需要用到的设备包括无线接入点、无线路由器、无线网卡和天线等。

（1）无线接入点

无线接入点就是通常所说的 AP，也被称为无线访问点。它是大多数无线网络的中心设备。无线路由器、无线交换机和无线网桥等设备都是无线接入点定义的延伸，因为它们所

提供的最基础作用仍是无线接入。AP 在本质上是一种提供无线数据传输功能的集线器，它在无线局域网和有线网络之间接收、缓冲存储和传输数据，以支持一组无线用户设备。接入点通常是通过一根标准以太网线连接到有线主干线路上，并通过内置或外接天线与无线设备进行通信，无线 AP 通常只有一个网络接口，如图 4-12（a）所示。

（2）无线路由器

无线路由器是一种带路由功能的无线接入点，它主要应用在家庭及小企业。无线路由器具备无线 AP 的所有功能，如支持 DHCP、防火墙、支持 WEP/WPA 加密等，除此之外还包括了路由器的部分功能，如网络地址转换（NAT）功能，通过无线路由器能够实现跨网段数据的无线传输，从而实现 ADSL 或小区宽带的无线共享接入。

无线路由器通常包含一个若干端口的交换机，可以连接若干台使用有线网卡的计算机，从而实现有线和无线网络的顺利过渡，如图 4-12（b）所示。

（a）无线接入点

（b）无线路由器

图4-12　无线接入点和无线路由器

（3）无线网卡

使用无线网络接入技术的网卡可以统称为无线网卡，它们是操作系统与天线之间的接口，用来创建透明的网络连接。其接口一般有 USB、PCMCIA、PCI 和 MINI-PCI、CF/CFII 等形式，如图 4-13、图 4-14、图 4-15 所示。

图 4-13　USB 接口无线网卡

图 4-14　PCI 接口无线网卡

图 4-15　PCMCIA 接口无线网卡

MINI-PCI 无线网卡即笔记本电脑中内置式无线网卡，目前大多数笔记本电脑均使用这种无线网卡，如图 4-16 所示。其优点是无须占用 PC 卡或 USB 插槽，老式的笔记本电脑是直接将芯片焊接在主板上的。

CF 无线网卡是应用在 PDA、PPC 等移动设备或终端上的网卡，其特点是体积很小且可在设备上直接插拔，如图 4-17 所示。目前的 CF 卡一般是 TypeⅡ（CFⅡ）的接口。

图 4-16　MINI-PCI 无线网卡

图 4-17　CF 无线网卡

（4）天线

无线天线相当于一个信号放大器，主要用来解决无线网络传输中因传输距离、环境影响等造成的信号衰减。与接收广播电台时增加天线长度后声音会清晰很多原理相同，无线设备（如 AP）本身的天线，由于国家对功率有一定限制，它只能传输较短的距离，当超出这个有限的距离时，可以通过外接天线来增强无线信号，达到延伸传输距离的目的。

5．无线局域网的组网方式

无线局域网采用单元结构，将各个系统分成许多单元，每个单元称为一个基本服务组，服务组的组成结构主要有两种形式：无中心无线网络拓扑结构和有中心无线网络拓扑结构。

无中心无线网络拓扑结构如图 4-18 所示，网络中任意两个站点间均可直接通信，一般采用公用广播信道，各站点可竞争公用信道，而信道接入控制协议大多采用 CSMA 类型的多址接入协议，一般适用于较小规模的网络。

有中心无线网络拓扑结构如图 4-19 所示，网络中要求有一个无线站点作为中心，其他站点通过中心 AP 进行通信。此种拓扑结构网络风险高，中心站点的故障易导致整个网络瘫痪。

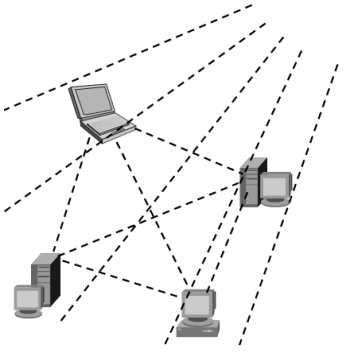


图 4-18　无中心无线网络拓扑结构

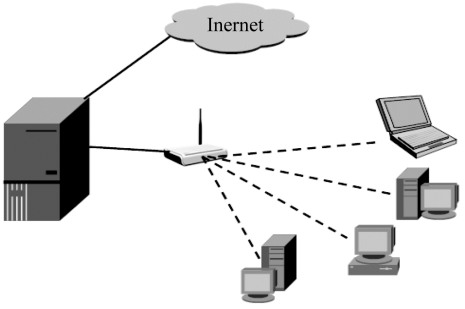


图 4-19　有中心无线网络拓扑结构

在实际无线网络组网中，常常将无线网络与有线主干网络结合起来，中心站点充当无

线网络与有线主干网的桥接器，如图 4-20 所示。

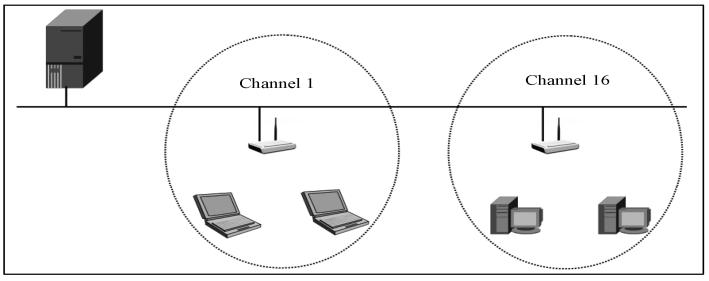


图 4-20　无线网络与有线主干网络结合

4.6　交换式局域网

在交换式局域网中，所有端点都要通过交换机连接起来，交换机为端点提供存储转发和路由选择功能，使端点间能沿着指定的路径传输数据，而不是像共享式局域网那样把数据广播到每个节点。

交换式局域网的核心是交换机，交换机提供了多个端口。高档交换机可以提供数十个乃至上百个交换端口，每个端口可以连入网段 Hub 或单个站点。交换机提供大容量的动态交换带宽，可在多个节点间建立多个并行的通信链路。节点间沿指定路径转发报文，使竞争式共享信道转变为独享式信道，这相当于实现了一个并行局域网系统。多对不同源端点和目的端点之间可同时进行通信，而不会发生冲突，大大提高了局域网的可用带宽，减少了局域网延迟。

在高档交换机中，其动态交换带宽可达 GB 数量级，允许上百个 10 Mbps 信息同时输入交换机，并同时建立上百个实时通信链路。

4.6.1　交换式局域网的基本特点

交换式以太网的核心设备是以太网交换机，通常有十几个端口。因此，以太网交换机实质上就是一个多端口的网桥，工作在数据链路层。此外，以太网交换机的每个端口都直接与主机相连，工作在全双工模式。以太网交换机由于使用了专用的交换机芯片，因此其交换速率较高。

对于普通 10Mbps 的共享式以太网，若共有 N 个用户，则每个用户占有的平均带宽只有总带宽（10Mbps）的 $1/N$。在使用以太网交换机时，虽然每个端口到主机的数据率还是 10Mbps，但用户在通信时是独占而不是和其他网络用户共享传输媒体的带宽，因此拥有 N 对端口的交换机的总容量为 $N\times$10Mbps。这正是交换机的最大优点。

交换以太网采用存储转发技术或直通技术来实现信息帧的转发。存储转发技术是将需发送的信息帧完全接收并存放到输入缓存后再发送至目的端口；而直通技术是在接收到信

息帧时和交换式集线器中的目的地址表相比较，查找到目的地址后就直接将信息帧发送到目的端口。

交换式局域网是以交换机为中心的星型结构。交换机下行连接到局域网用户设备和局域网主服务器，上行连接到高速主干网上，如千兆以太网交换机。当连接到高速主干网时，LAN 交换机应具有连接高速主干网的相应端口或模块，这种连接方式主要用于解决大型局域网中主干网或服务器的瓶颈问题。在主干网中，主交换机通常具有千兆以太网的高速端口及部分路由器功能，能防止广播风暴及隔离故障，并有较强的容错能力。

总之，高速的交换式局域网可以提供独享带宽、短延迟和易管理的局域网性能，可支持多媒体通信。

4.6.2 交换机的基本工作原理

交换机属于数据链路层设备，可以识别数据包中的 MAC 地址信息，根据 MAC 地址进行数据转发，并将这些 MAC 地址与对应的端口记录在自己内部的一个地址表中。地址表中记录的是 MAC 地址与交换机端口号的对应关系等信息，交换机的工作是围绕着这个 MAC 地址表来进行的。

当交换机控制电路从某一端口收到一个数据帧后，将立即在其内存的地址表中进行查找，以确认该目的地址的网卡连接在哪一个端口，然后将该帧转发至该端口。如果在地址表中没有找到该物理地址，也就是说，该目的物理地址是首次出现，则将其广播到所有端口。拥有该物理地址的网卡在接收到该广播帧后，将会立即做出应答，从而使交换机将其端口号物理地址添加到交换机中的地址表中。

在交换机刚刚打开电源时，其地址表是一片空白。那么，交换机的地址表是怎样建立起来的呢？交换机根据以太网帧中的源物理地址来更新地址表。当一台计算机打开电源后，安装在该计算机中的网卡会定期发出空闲包或信号，交换机即可据此得知它的存在及其物理地址。由于交换机能够自动根据收到的以太网帧中的源物理地址更新地址表的内容，所以交换机使用的时间越长，地址表中存储的物理地址就越多，未知的物理地址就越少，因而广播包就越少，速度就越快。

交换机不会永久性地记住所有的端口号物理地址关系，由于交换机中的内存毕竟有限，因此，能够记忆的物理地址数量也是有限的。在交换机内有一个忘却机制，当某一物理地址在一定时间内不再出现（该时间由网络工程师设定，默认为 300s）时，交换机自动将该地址从地址表中清除，当下一次该地址重新出现时，交换机将其作为新地址处理，重新记入地址表中。

4.6.3 交换机的分类

由于交换机具有许多优越性，所以它的应用和发展速度远远高于集线器，出现了各种类型的交换机，主要是为了满足各种不同应用环境需求。根据划分标准的不同，局域网交换机可划分为多种不同的类型。

1．从网络覆盖范围划分

（1）广域网交换机

广域网交换机主要是应用于电信城域网互联、互联网接入等领域的广域网中，提供通信用的基础平台。

（2）局域网交换机

局域网交换机应用于局域网络，用于连接终端设备，如服务器、工作站、集线器、路由器、网络打印机等网络设备，提供高速独立通信通道。

2．根据传输介质和传输速度划分

根据交换机使用的网络传输介质及传输速度的不同，一般可以将局域网交换机分为以太网交换机、快速以太网交换机、千兆（G 位）以太网交换机、10 千兆（10G 位）以太网交换机、FDDI 交换机、ATM 交换机和令牌环交换机等。

（1）以太网交换机

这里所指的“以太网交换机”，是指带宽在 100Mbps 以下的以太网所用交换机，其实下面所述“快速以太网交换机”、“千兆以太网交换机”和“10 千兆以太网交换机”也是以太网交换机，只不过它们所采用的协议标准或者传输介质不一样，当然其接口形式也可能不一样。

以太网交换机的档次比较齐全，应用领域也非常广泛，在大大小小的局域网都可以见到它们的踪影。以太网包括三种网络接口：RJ-45、BNC 和 AUI，所用的传输介质分别为双绞线、细同轴电缆和粗同轴电缆。由于双绞线类型的 RJ-45 接口在网络设备中非常普遍。所以一般是在 RJ-45 接口的基础上为了兼顾同轴电缆介质的网络连接，配上 BNC 或 AUI 接口。如图 4-21 所示为一款带有 RJ-45 和 AUI 接口的以太网交换机产品示意图。

（2）快速以太网交换机

这种交换机用于 100Mbps 快速以太网。快速以太网是一种在普通双绞线或者光纤上实现 100Mbps 传输带宽的网络技术。一般来说，这种快速以太网交换机通常所采用的介质也是双绞线，有的快速以太网交换机为了兼顾与其他光传输介质的网络互联，或许会留有少数的光纤接口“SC”。如图 4-22 所示为一款快速以太网交换机产品示意图。

图 4-21　兼有 RJ-45 和 AUI 接口的以太网交换机产品示意图

图 4-22　快速以太网交换机产品示意图

（3）千兆以太网交换机

千兆以太网交换机是用于目前较新的一种网络——千兆以太网中，也有人把这种网络称为“吉位（GB）以太网”，那是因为它的带宽可以达到 1000Mbps。它一般用于一个大型网络的骨干网段，所采用的传输介质有光纤、双绞线两种，对应的接口为“SC”和“RJ-45”接口两种。如图 4-23 所示为两款千兆以太网交换机产品示意图。

（a）

（b）

图4-23　千兆以太网交换机产品示意图

（4）10 千兆以太网交换机

10千兆以太网交换机主要是为了适应10千兆以太网络的接入，它一般用于骨干网段上，采用的传输介质为光纤，其接口方式也为光纤接口，同样这种交换机也可称为“10Gbps 以太网交换机”。目前 10Gbps 以太网技术还处于初始阶段，价格也非常昂贵（一般要 2～9 万美元），所以 10Gbps 以太网在实际应用中还不是很普遍。如图 4-24 所示为一款 10 千兆以太网交换机产品示意图，从图中可以看出它全部采用了光纤接口。

图 4-24　10 千兆以太网交换机产品示意图

3．根据应用层次划分

根据交换机所应用的网络层次，将网络交换机划分为企业级交换机、校园网交换机、部门级交换机和工作组交换机、桌面型交换机五种。

（1）企业级交换机

企业级交换机属于高端交换机，一般采用模块化的结构，可作为企业网络骨干构建高速局域网，所以它通常用于企业网络的顶层。

企业级交换机可以提供用户化定制、优先级队列服务和网络安全控制，并能很快适应数据增长和改变的需要，从而满足用户的需求。对于有更多需求的网络，企业级交换机不仅能传送海量数据和控制信息，更具有硬件冗余和软件可伸缩性特点，保证网络的可靠运行。这种交换机从它所处的位置可以清楚地看出它自身的要求非同一般，起码在带宽、传输速率及背板容量上要比一般交换机高出许多，所以企业级交换机一般都是千兆以上以太网交换机。企业级交换机所采用的端口一般都为光纤接口，这主要是为了保证交换机高速率传输。目前，什么样的交换机可称为企业级交换机还没有一个明确的标准，通常认为，如果是作为企业的骨干交换机，能支持 500 个信息点以上大型企业应用的交换机为企业级交换机，如图 4-25 所示的是友讯的一款模块化千兆以太网交换机，它属于企业级交换机范畴。

图 4-25　模块化千兆以太网交换机产品示意图

企业交换机还可以接入一个大底盘。这个底盘产品通常支持许多不同类型的组件，如快速以太网和以太网中继器、FDDI 集中器、令牌环 MAU 和路由器。企业交换机在建设企业级别的网络时非常有用，尤其是对需要支持一些网

络技术和以前的系统。基于底盘设备通常有非常强大的管理特征，因此非常适合于企业网络的环境。

（2）校园网交换机

校园网交换机主要应用于较大型网络，且一般作为网络的骨干交换机。这种交换机具有快速数据交换能力和全双工能力，可提供容错等智能特性，还支持扩充选项及第三层交换中的虚拟局域网（VLAN）等多种功能。

这种交换机通常用于分散的校园网而得名，其实它不一定要应用在校园网络中，只表示它主要应用于物理距离分散的较大型网络中。因为校园网比较分散，传输距离比较长，所以在骨干网段上，这类交换机通常采用光纤或者同轴电缆作为传输介质，交换机当然也就需提供 SC 光纤接口和 BNC 或者 AUI 同轴电缆接口。

（3）部门级交换机

部门级交换机是面向部门级网络使用的交换机，它较前面两种的网络规模要小得多。这类交换机可以是固定配置，也可以是模块配置，一般除了常用的 RJ-45 双绞线接口外，还带有光纤接口。

部门级交换机一般具有较为突出的智能型特点，支持基于端口的 VLAN（虚拟局域网），可实现端口管理，可任意采用全双工或半双工传输模式，可对流量进行控制，有网络管理的功能，可通过 PC 的串口或经过网络对交换机进行配置、监控和测试。如果作为骨干交换机，则一般认为支持 300 个信息点以下中型企业的交换机为部门级交换机。如图 4-26 所示为一款部门级交换机产品示意图。

（4）工作组交换机

工作组交换机是传统集线器的理想替代产品，一般为固定配置，配有一定数目的 10Base-T 或 100Base-TX 以太网接口。交换机按每一个包中的 MAC 地址相对简单地决策信息转发，这种转发决策一般不考虑包中隐藏的其他信息。与集线器不同的是交换机转发延迟很小，操作接近单个局域网性能，远远超过了普通桥接互联网络之间的转发性能。

工作组交换机一般没有网络管理的功能，如果是作为骨干交换机则一般认为支持 100 个信息点以内的交换机为工作组交换机。如图 4-27 所示为一款快速以太网工作组交换机产品示意图。

图 4-26　部门级交换机产品示意图

图 4-27　工作组交换机产品示意图

（5）桌面型交换机

桌面型交换机是最常见的一种低档交换机，它区别于其他交换机的一个特点是支持的每个端口 MAC 地址很少，通常端口数也较少，只具备最基本的交换机特性，当然价格也是最便宜的。

这类交换机虽然在整个交换机中属于最低档的，但是相比集线器来说它还是具有交换

机的通用优越性，况且有许多应用环境也只需这些基本的性能，所以它的应用还是相当广泛的。它主要应用于小型企业或中型以上企业办公桌面。在传输速度上，目前桌面型交换机大都提供多个具有 10/100Mbps 自适应能力的端口。如图 4-28 所示为两款不同品牌型号的桌面型交换机产品示意图。

（a）　　（b）

图 4-28　桌面型交换机产品示意图

4．根据交换机的结构划分

如果按交换机的端口结构来分，交换机大致可分为固定端口交换机和模块化交换机两种不同的结构。其实还有一种是两者兼顾，那就是在提供基本固定端口的基础之上再配备一定的扩展插槽或模块。

（1）固定端口交换机

固定端口顾名思义就是它所带的端口是固定的，如果是 8 端口的，就只能有 8 个端口，再不能添加。16 个端口也就只能有 16 个端口，不能再扩展。目前这种固定端口的交换机比较常见，端口数量没有明确的规定，一般的端口标准是 8 端口、16 端口和 24 端口。目前交换机的端口比较复杂，非标准的端口数主要有 4 端口、5 端口、10 端口、12 端口、20 端口、22 端口和 32 端口等。

固定端口交换机虽然相对来说价格便宜一些，但由于它只能提供有限的端口和固定类型的接口，因此，无论从可连接的用户数量上，还是从可使用的传输介质上来讲都具有一定的局限性，但这种交换机在工作组中应用较多，一般适用于小型网络、桌面交换环境。如图 4-29 所示分别是一款 16 端口和 24 端口的交换机产品示意图。

（a）　　（b）

图 4-29　16 端口和 24 端口交换机产品示意图

固定端口交换机因其安装架构又分为桌面式交换机和机架式交换机。机架式交换机更易于管理，更适用于较大规模的网络，它的结构尺寸要符合 19 英寸国际标准，用来与其他交换设备或者是路由器、服务器等集中安装在一个机柜中。而桌面式交换机，由于只能提供少量端口且不能安装于机柜内，所以，通常只用于小型网络。如图 4-30 所示为一款机架

图4-30　机架式固定端口交换机产品示意图

式固定端口交换机产品示意图。

（2）模块化交换机

模块化交换机拥有更大的灵活性和可扩充性，用户可任意选择不同数量、不同速率和不同接口类型的模块，以适应千变万化的网络需求。而且，机箱式交换机大都有很强的容错能力，支持交换模块的冗余备份，并且往往拥有可热插拔的双电源，以保证交换机的电力供应。在选择交换机时，应按照需要和经费综合考虑选择机箱式或固定方式。一般来说，企业级交换机应考虑其扩充性、兼容性和排错性，因此，应当选用机箱式交换机；而骨干交换机和工作组交换机则由于任务较为单一，故可采用简单明了的固定式交换机。如图 4-31 所示为一款模块化快速以太网交换机产品示意图，其中具有 4 个可拨插模块，可根据实际需要灵活配置。

5．根据交换机工作的协议层划分

网络设备都是对应工作在 OSI/RM 这一开放模型的一定层次上，工作的层次越高，说明其设备的技术性越高，性能也越好，档次也就越高。交换机也一样，随着交换技术的发展，交换机由原来工作在 OSI/RM 的第二层，发展到现在有可以工作在第四层的交换机出现，所以根据交换机工作的协议层，可将交换机分为第二层交换机、第三层交换机和第四层交换机。

（1）第二层交换机

第二层交换机是对应于 OSI/RM 的第二协议层来定义的，因为它只能工作在 OSI/RM 开放体系模型的第二层——数据链路层。第二层交换机依赖于链路层中的信息（如 MAC 地址）完成不同端口数据间的线速交换，主要功能包括物理编址、错误校验、帧序列以及数据流控制。

这是较早的交换技术产品，目前桌面型交换机一般属于这个类型，桌面型交换机一般来说所承担的工作复杂性不是很强，又处于网络的基层，所以也就只需要提供最基本的数据链接功能即可。目前第二层交换机应用最为普遍（主要是价格便宜，功能符合中、小企业实际应用需求），一般应用于小型企业或中型以上企业网络的桌面层次。如图 4-32 所示为一款第二层交换机的产品。要说明的是，所有的交换机在协议层次上来说都是向下兼容的，也就是说所有的交换机都能够工作在第二层。

图 4-31　模块化快速以太网交换机产品示意图

图 4-32　第二层交换机产品示意图

（2）第三层交换机

第三层交换机同样是对应于 OSI/RM 开放体系模型的第三层——（网络层）来定义的，也就是说这类交换机可以工作在网络层，它比第二层交换机更加高档，功能更加强大。第三层交换机因为工作于 OSI/RM 模型的网络层，所以它具有路由功能，将 IP 地址信息提供给网络路径选择，并实现不同网段间数据的线速交换。当网络规模较大时，可以根据特殊应用需求划分为独立的 VLAN 网段，以减小广播所造成的影响。

通常这类交换机采用模块化结构，以适应灵活配置的需要。在大中型网络中，第三层交换机已经成为基本配置设备。如图 4-33 所示为 3COM 公司生产的一款第三层交换机产品。

（3）第四层交换机

第四层交换机是采用第四层交换技术而开发出来的交换机产品，当然它工作于 OSI/RM 模型的第四层，即传输层，直接面对具体应用。第四层交换机支持的协议是各种各样的，如 HTTP、FTP、Telnet、SSL 等。

在第四层交换中为每个供搜寻使用的服务器组设立虚 IP 地址（VIP），每组服务器支持某种应用。在域名服务器（DNS）中存储的每个应用服务器地址是 VIP，而不是真实的服务器地址。当某用户申请应用时，一个带有目标服务器组的 VIP 连接请求（如一个 TCPSYN 包）发给服务器交换机。服务器交换机在组中选取最好的服务器，将终端地址中的 VIP 用实际服务器的 IP 取代，并将连接请求传给服务器。这样，同一区间所有的包由服务器交换机进行映射，在用户和同一服务器间进行传输。如图 4-34 所示为一款第四层交换机产品。

图 4-33　第三层交换机产品示意图

图 4-34　第四层交换机产品示意图

第四层交换技术相对原来的第二层交换技术、第三层交换技术具有明显的优点，从操作方面来看，第四层交换是稳固的，因为它将包控制在从源端到宿端的区间中。另外，路由器或第三层交换，只针对单一的包进行处理，不清楚上一个包从哪来，也不知道下一个包的情况。它们只是检测包报头中的 TCP 端口数字，根据应用建立优先级队列，路由器根据链路和网络可用的节点决定包的路由；而第四层交换机则是在可用的服务器和性能基础上先确定区间。目前由于这种交换技术尚未真正成熟且价格昂贵，所以，第四层交换机在实际应用中还较少见。

6．根据是否支持网络管理功能划分

如果按交换机是否支持网络管理功能，交换机又可分为“网管型”和“非网管型”两大类。

网管型交换机的任务就是使所有的网络资源处于良好的状态。网管型交换机产品提供

了基于终端控制口（Console）、基于 Web 页面以及支持 Telnet 远程登录网络等多种网络管理方式。因此网络管理人员可以对该交换机的工作状态、网络运行状况进行本地或远程的实时监控，纵观全局地管理所有交换端口的工作状态和工作模式。网管型交换机支持 SNMP 协议，SNMP 协议由一整套简单的网络通信规范组成，可以完成所有基本的网络管理任务，对网络资源的需求量少，具备一些安全机制。NMP 协议的工作机制非常简单，主要通过各种不同类型的消息，即 PDU（协议数据单位）实现网络信息的交换。但是网管型交换机相对下面所介绍的非网管型交换机来说，其价格要贵许多。

网管型交换机采用嵌入式远程监视（RMON）标准用于跟踪流量和会话，对决定网络中的瓶颈和阻塞点是很有效的。软件代理支持 4 个 RMON 组（历史、统计数字、警报和事件），从而增强了流量管理、监视和分析。统计数字是一般网络流量统计；历史是一定时间间隔内网络流量统计；警报可以在预设的网络参数极限值被超过时进行报警；事件代表管理事件。

还有网管型交换机提供基于策略的 QoS（Quality of Service）。策略是指控制交换机行为的规则，网络管理员利用策略为应用流分配带宽、优先级以及控制网络访问，其重点是满足服务水平协议所需的带宽管理策略及向交换机发布策略的方式。在交换机的每个端口处用来表示端口状态、半双工/全双工和 10BaseT/100BaseT 的多功能发光二极管（LED）以及表示系统、冗余电源（RPS）和带宽利用率的交换级状态 LED 形成了全面、方便的可视管理系统。目前大多数部门级以下的交换机多数都是非网管型的，只有企业级及少数部门级的交换机支持网管功能。如图 4-35 所示为两款网管型交换机。

（a）　　（b）

图 4-35　网管型交换机产品示意图

4.6.4 交换机的技术指标

交换机的基本技术指标较多，这些技术指标全面地反映了交换机的技术性能及其主要功能，是用户选购产品时的重要参考依据。其中主要的技术指标如下。

1．端口数量

端口是指交换机连接网络传输介质的接口部分。目前交换机的端口大多数都是 RJ-45 端口，外观上与集线器的端口一样，交换机的端口主要有 8 端口、16 端口、24 端口及 48 端口。

2．端口速率

目前百兆带宽已经是网络发展的一个趋势，因此用户应尽量选择 10/100Mbps 自适应的

交换机。每个端口独享 10Mbps 或者 100Mbps 带宽。端口的实际速率并不只取决于交换机，还取决于网卡。

3．机架插槽数和扩展槽数

机架插槽数是指机架式交换机所能安插的最大模块数；扩展槽数是指固定配置式带扩展槽交换机所能安插的最大模块数。

4．背板带宽

背板是整个交换机的交通干线，类似于计算机的总线，它的值越大，则在各端口同时传输数据时，给每个端口提供的带宽也就越大，传输速率也就越大，交换机的性能也要高一些。一般情况下，每个端口平均分配的背板带宽需要在 100Mbps 以上。

5．支持的网络类型

一般情况下，固定配置式不带扩展槽的交换机仅能支持一种类型的网络，机架式交换机和固定配置式带扩展槽的交换机可以支持一种以上的网络。一台交换机所支持的网络类型越多，其可用性和可扩展性越强。

6．MAC 地址表大小

连接到局域网上的每个端口或设备都需要一个 MAC 地址，其他设备要用此地址来定位特定的端口及更新路由表和数据结构。一个交换机的 MAC 地址表的大小反映了连接到该设备能支持的最大节点数。

7．最大可堆叠数

“可堆叠”是指交换机可以通过堆叠模块，将两台或两台以上的交换机逻辑上合并成一台交换机，相当于扩展了端口数量，背板带宽也同步扩展。此参数说明了一个堆叠单元中所能提供最大端口密度与信息点的连接能力。堆叠与级联不同，堆叠相当于并联电路，级联相当于串联电路。

8．可网管

网管是指网络管理员通过网络管理程序对网络上的资源进行集中化的管理，包括配置管理、性能和记账管理、问题管理、操作管理和变化管理等。一般交换机厂商会提供管理软件或第三方管理软件来远程管理交换机。

可网管交换机是指符合 SNMP 规范（简单网络管理协议）、能够通过软件手段进行诸如查看交换机的工作状态、开通或封闭某些端口等管理操作的交换机。网络管理界面分为命令行方式（CLI）与图形用户界面（GUI）方式，不同的管理程序反映了该设备的可管理性及可操作性。

9．最大 SONET 端口数

SONET（同步光传输网络）是一种高速同步传输网络规范，最大速率可达 2.5Gbps。一台交换机的最大 SONET 端口数是指这台交换机的最大传输速率的 SONET 端口数。

10．支持的协议和标准

交换机支持的协议和标准内容，直接决定了交换机的网络适应能力。局域网交换机所支持的协议和标准内容，直接决定了交换机的网络适应能力。这些协议和标准一般是指由国际标准化组织所制定的联网规范和设备标准。由于交换机工作在第二层或第三层上，工作中要涉及第三层以下的各类协议。

11．缓冲区大小

缓冲区大小有时又称为包缓冲区大小，是一种队列结构，被交换机用来协调不同网络设备之间的速度匹配问题。突发数据可以存储在缓冲区内，直到被慢速设备处理为止。缓冲区大小要适度，过大的缓冲空间会影响正常通信状态下数据包的转发速率（因为过大的缓冲空间需要相对多一点的寻址时间），并增加设备的成本。而过小的缓冲空间在发生拥塞时又容易丢包出错。所以，适当的缓冲空间加上先进的缓冲调度算法是解决缓冲问题的合理方式。

习　题　4

一、填空题

1．局域网是一个允许很多彼此_____在适当的区域内、以适当的_____直接进行沟通的数据通信系统。

2．局域网在网络拓扑结构上主要采用了_____、_____和_____；在网络传输介质上主要使用_____、_____与_____。

3．按照 IEEE 802 标准，局域网的体系结构由三层协议构成，即_____、_____和_____。

4．“媒体访问控制层”和“逻辑链路控制层”这两层相当于 OSI 七层参考模型中的第_____层，即_____。

5．介质访问控制（MAC）方法是在局域网中对数据_____进行访问管理的方法。

6．通常，可将信道分配方法划分为两类：_____和_____。

7．冲突检测/载波监听（CSMA/CD）是以太网中采用的介质访问控制方法，其中 CS 是_____，MA 是_____，CD 是_____。

8．组成一个局域网有三大要素：_____、_____及_____。

9．通常组建局域网需要的网络硬件主要是_____、_____、网络适配器（网卡）、_____及传输介质等。

10．在局域网上使用的网络软件主要是_____、_____和网络应用软件。

11．对等网也可以说成就是不要_____的局域网，它是一个_____网络系统。

12．现在广泛使用的局域网技术主要有_____、_____、_____、FDDI 网络及 ATM 网络。

13．ATM 是高速分组交换技术，其基本数据传输单元是_____。

14．光纤分布数据接口（FDDI）标准是由美国国家标准协会建立的一套标准，它使用基本令牌的_____体系结构，以_____为传输介质。

15．无线局域网 WLAN 是_____与_____相结合的产物，移动通信技术的飞速发展也为无线接入提供了基础。WLAN 可提供移动接入的功能，一般采用_____和_____。

16．一般来说，组建无线局域网需要用到的设备包括_____、_____、_____和天线等。

17．无线局域网采用单元结构，将各个系统分成许多单元，每个单元称为一个基本服务组，服务组的组成结构主要有两种形式：_____和_____。

18．根据交换机所应用的网络层次，将网络交换机划分为_____、校园网交换机、_____和_____、_____五种。

19．根据交换机工作的协议层，可将交换机分为_____、_____和_____。

二、选择题

1．从达到的目的角度来看，网络互联包含了 3 个不同层次的内容，它们是（　　）。

A．互通、互联、交换　　B．互联、互通、互操作

C．互联、互通、共享　　D．互通、互联、连通

2．网络互联主要在（　　）中实现。

A．物理层、数据链路层、网络层

B．物理层、数据链路层、表示层

C．数据链路层、网络层、高层

D．物理层、数据链路层、会话层

3．在下列传输介质中，在单个建筑物内局域网通常使用的传输介质是（　　）。

A．双绞线　　B．同轴电缆

C．光纤　　D．无线介质

4．交换机工作于 OSI 参考模型的（　　）。

A．物理层　　B．数据链路层

C．网络层　　D．高层

5．路由器工作于 OSI 参考模型的（　　）。

A．物理层　　B．数据链路层

C．网络层　　D．高层

6．计算机网络中选择最佳路由的网络连接设备是（　　）

A．路由器　　B．交换机

C．网卡　　D．集线器

7．交换式局域网的核心设备是（　　）。

A．路由器　　B．局域网交换机

C．集线器　　D．中继器

8．把计算机网络分为有线网和无线网的分类依据是（　　）。

A．地理位置　　B．传输介质

C．拓扑结构　　D．成本价格

9．网络中所连接的计算机在 10 台以内时，多采用（　　）。

A．对等网　　B．基于服务器的网络

C．点对点网络　　D．小型 LAN

10．客户机/服务器模式的英文写法是（　　）。

A．Slave/Master　　B．Guest/Server

C．Guest/Master　　D．Client/Server

11．局域网和广域网相比最显著的区别是（　　）。

A．前者网络传输速率快　　B．后者吞吐量大

C．前者传输范围小　　D．后者可以传输的数据类型多于前者

12．“覆盖 50km 以上，传输速度较快”，上述特征所属的网络类型是（　　）。

A．广域网　　B．局域网　　C．互联网　　D．城域网

13．10Base-T 网络中，其传输介质为（　　）。

A．细缆　　B．粗缆　　C．微波　　D．双绞线

14．一座办公大楼内各个办公室中的微机进行联网，这个网络属于（　　）。

A．WAN　　B．LAN　　C．MAN　　D．GAN

15．在局域网的硬件系统中，网络用户最终的操作平台称为（　　）。

A．服务器　　B．工作站

C．显示设备　　D．网络连接器

三、简答题

1．什么是局域网？局域网有何特征？

2．介质访问控制方法的主要内容有哪些？

3．局域网的工作模式有哪几种?

4．什么是对等网？对等网有何技术特点？

5．B/S 结构的工作模式有何优缺点？

6．什么是无线局域网？其特点有哪些？

7．简述几种无线传输介质的区别。

8．交换机的主要性能指标有哪些？

9．简述交换机的工作原理。

10．交换机的技术指标有哪些？

第5章 网络管理与安全

内容摘要

- 网络管理
- 网络安全
- 网络安全机制
- 防火墙技术

学习目标

- 理解网络管理的功能和协议
- 掌握网络常见故障排除方法
- 掌握网络安全基本知识
- 理解安全防范技术、加密技术和安全认证技术
- 掌握防火墙的概念、作用、分类及部署

随着网络技术的普及，网络的安全性显得更加重要。这是因为怀有恶意的攻击者可能窃取、篡改网络上传输的信息，通过网络非法入侵获取储存在远程主机上的机密信息，或构造大量的数据报文汇款占用网络资源，阻止其他合法用户正常使用等。然而，网络作为开放的信息系统必然存在诸多潜在的安全隐患，因此，网络安全技术作为一个独立的领域越来越受到人们的关注。

随着全球信息高速公路的建设和发展，个人、企业乃至整个社会对信息技术的依赖程度越来越大，一旦网络系统安全受到严重威胁，不仅会对个人、企业造成不可避免的损失，严重时将会给企业、社会乃至整个国家带来巨大的经济损失。因此，提高对网络安全重要性的认识，增强防范意识，强化防范措施，不仅是各个企业要重视的问题，也是保证信息产业持续稳定发展的重要保证和前提条件。

5.1 网 络 管 理

5.1.1 网络管理概述

局域网建成并投入使用后，如何管好、用好网络，使网络保持在一个稳定的工作状态，尽量发挥其最大作用，就成为网络管理员的一项基本工作。网络系统的管理涉及网络软硬件系统管理、辅助设施管理及用户管理等方面的因素，工作复杂但又十分重要。

随着网络事业的蓬勃发展，网络对于人们的意义越来越重要。网络环境已经成为一个现代化办公场所的基础，成为维持业务正常运转的基本条件。人们对网络的依赖程度不断增加的同时，网络本身的功能及结构也变得越来越复杂。计算机网络由一系列的计算机、数据通信设备等硬件系统，以及应用、管理软件系统所构成。随着网络规模的扩大，以及网络资源的种类和数量的增多，网络管理工作也显得尤为重要。网络需要人们进行管理和维护，才能保持正常运行，才能为用户提供更好的网络服务。

5.1.2 网络管理中心与网络管理功能

1．网络管理中心

网络管理中心，通常由一组功能不同的控制设备组成，它们指挥和控制网络中心的其他设备一起完成网络管理的任务。网络管理中心向网络中心的各种设备发出各种控制命令，这些设备执行命令并返回结果。除此之外，网络管理中心还可以直接收集其他设备定期或随时发来的各种统计信息和报警报告，对其进行分析，并确定进一步的控制操作。

网络管理中心的配置通常与网络管理方式及网络规模密切相关，网络管理的方式主要有集中式管理和分布式管理两类，前者适合于网络管理中心或者直接使某台设备兼含网管功能时使用；当网络规模较大、网络设备分布较广时，由于管理信息量的增多，通常采用后者管理，并用一组网络管理中心协同进行管理。每个网络管理中心负责实施一定区域和一定层次的网络管理任务。

当网络中需要设置网络管理中心时，其核心设备是一台或几台网管服务器，网管服务器配置有海量存储设备，保存必要的系统软件映像、数据库信息和实用开发软件等。网管服务器通过与其他网络设备进行通信，自动执行网络的管理和控制，同时还向操作人员显示网络运行状态，进行报警信息和统计信息的显示和打印等。鉴于网络管理中心所处的重要地位，其中的设备通常采用双机切换工作方式，以确保网络管理的高可靠性。

2．网络管理功能

一个功能完善的网络管理系统，对网络的使用有着极为重要的意义。它通常具有以下 5 个方面的功能。

（1）配置管理

配置管理是指对网络中每个设备的功能、相互间的连接关系和工作参数进行监测、控制和配置调整，它反映了网络状态的变化。网络是经常需要变化的，需要调整网络配置的原因很多，主要有以下几点。

① 为向用户提供满意的服务，网络必须根据用户需求的变化，增加新的资源与设备，调整网络的规模，以增强网络的服务能力。

② 网络管理系统在检测到某个设备或线路发生故障时，以及在故障排除过程中都将会影响到部分网络的结构。

③ 通信子网中某个节点的故障会造成网络上节点的减少与路由的改变。

对网络配置的改变可能是临时性的，也可能是永久性的。网络管理系统必须有足够的手段来支持这些改变，不论这些改变是长期的还是短期的。有时甚至要求在短期内自动修改网络配置，以适应突发性事件的需要。

配置管理就是用来识别、定义、初始化、控制与监测通信网中的管理对象。配置管理是网络管理中对管理对象的变化进行动态管理的核心，当配置管理软件接到网络管理员或其他管理功能设施的配置变更请求时，配置管理服务首先确定管理对象的当前状态并给出变更合法性的确认，然后对管理对象进行变更操作，最后要验证变更确实已经完成。

（2）故障管理

故障管理是用来维持网络的正常运行的。网络故障管理包括及时发现网络中发生的故障和找出网络故障产生的原因，必要时启动控制功能来排除故障。控制功能包括诊断测试、故障修复或恢复、启动备用设备等。

故障管理是网络功能中与检测设备故障、差错设备的诊断、故障设备的恢复或故障排除有关的网络管理功能，其目的是保证网络能够提供连续、可靠的服务。

常用的故障管理工具有网络系统、协议分析器、电缆测试仪、冗余系统、数据档案和备份设备等。

（3）性能管理

网络性能管理活动是持续地评测网络运行中的主要性能指标，以检验网络服务是否达到了预定的水平，找出已经发生或潜在的瓶颈，报告网络性能的变化趋势，为网络管理决策提供依据。性能管理指标通常包括网络响应时间、吞吐量、费用和网络负载。

对于性能管理，通过使用网络性能监视器（硬件和软件），能够给出一定性能指示的直方图。利用这一信息，预测将来对硬件和软件的需求、潜在的需要改善的区域，以及潜在的网络故障。

（4）记账管理

记账管理主要是对用户使用网络资源的情况进行记录并核算费用。

在企业内部网中，内部用户使用网络资源并不需要交费，但是记账功能可以用来记录用户对网络的使用时间、统计网络的利用率与资源使用等内容。

通过记账管理，可以了解网络的真实用途，定义它的能力和制定策略，使网络更有效。

（5）安全管理

安全管理功能是用来保护网络资源安全。安全管理活动能够利用各种层次的安全防卫机制，使非法入侵事件尽可能少发生；能够快速检测未授权的资源使用，并查出侵入点，

对非法活动进行审查与追踪；能够使网络管理人员恢复部分受破坏的文件。

在安全管理中可以通过使用网络监视设备，记录使用情况，报告越权或提供对高危险行为的警报。作为一个网络管理员，应该意识到潜在的危险，并用一些方法减少这些危险，避免造成不良后果。

5.1.3 简单网络管理协议（SNMP）

国际上的网络协议有很多，除专门的标准化组织制定的一些协议外，一些网络发展比较早的机构和厂家，如 IBM 公司、Internet 组织和 DEC 公司，也制定了一些应用在各自网络上的管理协议，其中，最著名的和应用最广泛的是 Internet 组织的网络管理协议 SNMP。

1．SNMP 的概念

简单网络管理协议（SNMP）的体系结构是从早期的简单网关监控协议（SGMP）发展而来的，是 Internet 组织用来管理采用 TCP/IP 协议的互联网和以太网的。SNMP 的两个最显著的特点如下：

① 虽然 SNMP 是为在 TCP/IP 之上使用而开发的，但它的监测和控制活动是独立于 TCP/IP 的；

② SNMP 仅仅需要 TCP/IP 提供无链接的数据报传输服务。

所以，SNMP 很容易应用到其他网络中。

2．SNMP 的目标

SNMP 的目标是管理 Internet 中众多厂家生产的软、硬件平台，其提供了 5 类管理操作。

① get 操作：用于提取特定的网络管理信息。

② get-next 操作：通过遍历活动来提供强大的管理信息提取能力。

③ set 操作：用来对管理信息进行控制。

④ get response 处理：用于响应 get、get-next 及 set 操作，返回它们的操作结果。

⑤ trap（陷阱）操作：用来报告重要事件。

SNMP 的体系结构是围绕以下 4 个概念和目标进行设计的。

① 保持管理代理 Agent 的软件成本尽可能低。

② 最大限度地保持远程管理的功能，以便充分利用 Internet 的网络资源。

③ 体系结构必须能在将来需要时有扩充的余地。

④ 保持 SNMP 的独立性，不依赖于具体的计算机、网关和网络传输协议。

3．SNMP 的基本组成

SNMP 管理模型中有三个基本组成部分：管理代理（Agent）、管理进程（Manager）和管理信息库（MIB）。

（1）管理代理（Agent）

管理代理是一种软件，在被管理的网络设备中运行，负责执行管理进程的管理操作。管理代理直接操作本地信息库（MIB），如果管理进程需要，它可以根据要求改变本地信息

库或提取数据传回到管理进程。

每个管理代理拥有自己的本地 MIB，一个管理代理管理的本地 MIB 不一定具有 Internet 定义的 MIB 的全部内容，而只需要包括与本地设备或设施有关的管理对象。管理代理具有两个基本管理功能：① 从 MIB 中读取各种变量值；② 在 MIB 中修改各种变量值。这里的变量也就是管理对象。

（2）管理进程（Manager）

管理进程是一个或一组软件程序，一般运行在网络管理站（或网络管理中心）的主机上，它可以在 SNMP 的支持下命令管理代理执行各种管理操作。

管理进程完成各种网络管理功能，通过各设备中的管理代理对网络内的各种设备、设施和资源实施监测和控制。另外，操作人员通过管理进程对全网进行管理。因而管理进程也经常配有图形用户接口，以容易操作的方式显示各种网络信息，如给出网络中各管理代理的配置图等。有时管理进程也会对各管理代理中的数据集中存档，以备事后分析。

（3）管理信息库（MIB）

管理信息库（MIB）是一个概念上的数据库，由管理对象组成，每个管理代理管理 MIB 中属于本地的管理对象，各管理代理控制的管理对象共同构成全网的管理信息库。

管理信息库（MIB）的结构必须符合使用 TCP/IP 的 Internet 的管理信息结构（SMI）。这个 SMI 实际上是参照 OSI 的管理信息结构制定的。尽管两个 SMI 基本一致，但 SNMP 和 OSI 的 MIB 中定义的管理对象却并不相同。Internet 的 SMI 和相应的 MIB 是独立于具体的管理协议（包括 SNMP）的。

5.1.4 网络故障排除基础

随着网络规模的日益增大，网络应用越来越复杂，网络中的故障种类繁多且难以排查。掌握常见的故障排除手段和方法，是对网络维护人员的基本要求。

1．网络故障的分类

根据网络故障对网络应用的影响程度，网络故障一般分为连通性故障和性能故障两大类。连通性故障是指网络中断，业务无法进行，它是最严重的网络故障；性能故障指网络的性能下降，传输速率变慢，业务受到一定程度的影响，但并未中断。

不同的网络故障类型具有不同的故障原因。

（1）连通性故障

连通性故障的表现形式主要有以下几种。

① 硬件、介质、电源故障：硬件故障是引起连通性故障的最常见原因。网络中的网络设备是由主机设备、板卡、电源等硬件组成的，并由电缆等介质所连接起来的。如果设备遭到撞击，安装板卡时有静电，电缆使用错误，都可能会引起硬件损坏，从而导致网络无法连通。另外，人为性的电源中断，如交换机的电源线连接松脱，也是引起硬件连通性故障的常见原因。

② 配置错误：设备的正常运行离不开软件的正确配置。如果软件配置错误，则很可能导致网络连通性故障。目前网络协议种类众多且配置复杂。如果某一种协议的某一个参数

没有正确配置，都很有可能导致网络连通问题。

③ 设备间兼容性问题：计算机网络的构建需要许多网络设备，从终端 PC 到网络核心的路由器、交换机，同时网络也很可能是由多个厂商的网络设备组成的，这时，网络设备的互操作性显得十分必要。如果网络设备不能很好兼容，设备间的协议报文交互有问题，也会导致网络连通性故障。

（2）性能故障

也许网络连通性没有问题，但是可能某一天网络维护人员突然发现，网络访问速度慢了，或者某些业务的流量阻塞，而其他业务流量正常。这时，则意味着网络就出现了性能故障。一般来说，计算机网络性能故障主要原因如下。

① 网络拥塞：如果网络中某一节点的性能出现问题，都会导致网络拥塞。这时需要查找到网络的瓶颈节点，并进行优化，解决问题。

② 到目的地不是最佳路由：如果在网络中使用了某种路由协议，但在部署协议时并没有仔细规划，则可能会导致数据经次优路线到达目的网络。

③ 供电不足：确保网络设备电源达到规定的电压水平，否则会导致设备处理性能问题，从而影响整个网络。

④ 网络环路：在交换网络中如果有物理环路存在，则可能引发广播风暴，降低网络性能。而距离矢量路由协议也可能会产生路由环路。因此在交换网络中，一定要避免环路的产生，而在网络中应用路由协议时，也要选择没有路由环路的协议或采取措施来避免路由环路发生。

网络故障发生时，维护人员首先要判断是连通性故障还是性能故障，然后根据故障类型进行相应的检查。连通性故障首先检查网络设备的硬件，查看电源是否正常、电缆是否正确等。如果是性能问题，则重点从以上几个方面来考虑，查找具体的故障原因。

2．网络故障的一般解决步骤

前面基本了解了计算机网络故障的大致种类，那么，如何排除网络故障呢？建议采用系统化故障排除方法。故障排除系统化是合理地、一步一步找出故障原因，并解决故障的总体原则。它的基本方法是将可能的故障原因所构成的一个大集合缩减（或隔离）成几个小的子集，从而使问题的复杂度降低。

故障排除时，有序的方法有助于解决所遇到的任何困难，如图 5-1 所示给出了一般网络故障排除流程。

（1）故障现象观察。要想对网络故障做出准确的分析，首先应该能够完整清晰地描述网络故障现象，标示故障发生时间地点，故障所导致的后果，然后才能确定可能产生这些现象的故障根源或症结。因此，准确观察故障现象，对网络故障做出完整、清晰的描述是重要的一步。

（2）故障相关信息收集。本步骤是收集有助于查找故障原因的更详细的信息，主要有以下 3 种途径。

① 向受影响的用户、网络人员或其他关键人员提出问题。

② 根据故障描述性质，使用各种工具收集情况，如网络管理系统、协议分析仪、相关 display 和 debugging 命令等。

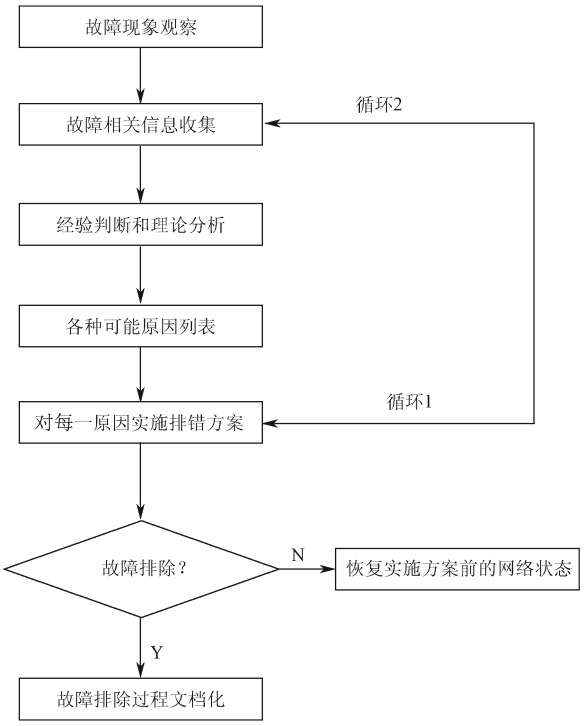


图 5-1　网络故障排除基本步骤

③ 测试目前网络性能，将测试结果与网络基线进行比较。

（3）经验判断和理论分析。利用前两个步骤收集到的数据，并根据自己以往的故障排除经验和所掌握的网络设备与协议的知识，来确定一个排错范围。通过范围的划分，就只需注意某一故障或与故障情况相关的那一部分产品、介质和主机。

（4）各种可能原因列表。根据潜在症结制订故障的排除计划，依据故障可能性高低的顺序，列出每一种认为可能的故障原因。从最有可能的症结入手，每次只做一次改动，然后观察改动的效果。之所以每次只做一次改动，是因为这样有助于确定针对特定故障的解决方法。如果同时做了两处或更多处改动，也许能够解决故障，但是难以确定最终是哪些改动消除了故障的症状，而且对日后解决同样的故障也没有太大的帮助。

（5）对每一原因实施排错方案。根据制订的故障排除计划，对每一个可能故障原因，逐步实施排除方案。在故障排除过程中，如果某一可能原因经验证无效，务必恢复到故障排除前的状态，然后再验证下一个可能原因。如果列出的所有可能原因都验证无效，那么就说明没有收集到足够的故障信息，没有找到故障发生点，则返回到第（2）步，继续收集故障相关信息，分析故障原因，再重复此过程，直到找出故障原因并且排除网络故障。

（6）观察故障排除结果。当对某一原因执行了排错方案后，需要对结果进行分析，判断问题是否解决，是否引入了新的问题。如果问题解决，那么就可以直接进入文档化过程；如果没有解决问题，那么就需要再次循环进行故障排除过程。

（7）循环进行故障排除过程。当一个方案的实施没有达到预期的排错目的时，便进入该步骤。这是一个努力缩小可能原因的故障排除过程。

在进行下一循环之前必须将网络恢复到实施方案前的状态。如果保留上一方案对网络的改动，很可能导致新的问题。例如，假设修改了访问列表但没有产生预期的结果，此时如果不将访问列表恢复到原始状态，就会导致出现不可预期的结果。

循环排错可以有两个切入点。

① 当针对某一可能原因的排错方案没有达到预期目的，循环进入下一可能原因制订排错方案并实施。

② 当所有可能原因列表的排错方案均没有达到排错目的，重新进行故障相关信息收集以分析新的可能故障原因。

（8）故障排除过程文档化。当最终排除了网络故障后，那么排除流程的最后一步就是对所做的工作进行文字记录。文档化过程绝不是一个可有可无的工作，原因如下。

① 文档是排错宝贵经验的总结，是“经验判断和理论分析”这一过程中最重要的参考资料。

② 文档记录了这次排错中网络参数所做的修改，这也是下一次网络故障应收集的相关信息。

文档记录主要包括以下几个方面。

① 故障现象描述及收集的相关信息。

② 网络拓扑图绘制。

③ 网络中使用的设备清单和介质清单。

④ 网络中使用的协议清单和应用清单。

⑤ 故障发生的可能原因。

⑥ 对每一可能原因制订的方案和实施结果。

⑦ 本次排错的心得体会。

⑧ 其他，如排错中使用的参考资料列表等。

5.1.5 故障排除常用方法

1．分层故障排除法

当模型的所有低层结构工作正常时，它的高层结构才能正常工作。层次化的网络故障分析方法有利于快速、准确地进行故障定位。

例如，在一个帧中继网络中，由于物理层的不稳定，帧中继链路经常出现间歇性中断。这个问题的直接表现是到达远程端点的路由总是出现间歇性中断。这使得维护人员第一反应是路由协议问题，然后凭借着这个感觉来对路由协议进行大量故障诊断和配置，其结果是可想而知的。如果能够从 OSI 模型的底层逐步向上来探究原因的话，维护人员将不会做出这个错误的假设，并能够迅速定位和排除问题。

在使用分层故障排除法进行故障排除时，具体每一层次的关注点有所不同。

（1）物理层：物理层负责通过某种介质提供到另一设备的物理连接，包括端点间的二进制流的发送与接收，完成与数据链路层的交互操作等功能。

物理层需要关注电缆、连接头、信号电平、编码、时钟和组帧，这些都是导致端口处

于 DOWN 状态的因素。

（2）数据链路层：数据链路层负责在网络层与物理层之间进行信息传输；规定了介质如何接入和共享；站点如何进行标识；如何根据物理层接收的二进制数据建立帧。

（3）网络层：网络层负责实现数据的分段封装与重组以及差错报告，更重要的是它负责信息通过网络的最佳路径的选择。

地址错误和子网掩码错误是引起网络层故障最常见的原因；网络地址重复是网络故障的另一个可能原因；另外，路由协议是网络层的一部分，也是排错重点关注的内容。

排除网络层故障的基本方法是：沿着从源到目的地的路径查看路由器上的路由表，同时检查那些路由器接口的 IP 地址是否正确。如果所需路由没有在路由表中出现，就应该检查路由器相关配置，然后手动添加静态路由或排除动态路由协议的故障以使路由表更新。

（4）传输层、应用层：传输层负责端到端的数据传输；应用层是各种网络应用软件工作的地方。如果确保网络层以下没有出现问题，而传输层或应用层出现问题，那么很可能就是网络终端软件出现故障，这时应该检查网络中的计算机、服务器等网络终端，确保应用程序正常工作，终端设备软、硬件运行良好。

2．分块故障排除法

各系列路由器和交换机等网络设备的配置文件中包括以下部分。

（1）管理部分（路由器名称、口令、服务、日志等）。

（2）端口部分（地址、封装、cost、认证等）。

（3）路由协议部分（静态路由、RIP、OSPF、BGP、路由引入等）。

（4）策略部分（路由策略、策略路由、安全配置）。

（5）接入部分（主控制台、Telnet 登录或哑终端、拨号等）。

（6）其他应用部分（语言配置、VPN 配置、QoS 配置等）。

上述分类给故障定位提供了一个原始框架，当出现一个故障案例现象时，可以把它归入上述某一类或某几类中，从而有助于缩减故障定位范围。

3．分段故障排除法

当一个故障涉及的范围较大时，可以通过分段故障排除法来将故障范围缩小。例如，如果两台路由器跨越电信部门提供的线路而不能相互通信时，可以按照以下分段，依次进行故障排除。

（1）主机到路由器 LAN 接口的一段。

（2）路由器到 CSU/DSU 接口的一段。

（3）CSU/DSU 到电信部门接口的一段。

（4）WAN 电路。

（5）CSU/DSU 本身问题。

（6）路由器本身问题。

在实际网络故障排错时，可以先采用分段法确定故障点，再通过分层或其他方法排除故障。

4．替换法

这是检查硬件是否存在问题最常用的方法。例如，当怀疑是网线问题时，更换一根好的网线试一试；当怀疑是接口模块有问题时，更换一个其他接口模块试一试。

5.2 网络安全的重要性

计算机网络的建立有效地实现了资源共享，但是资源共享和资源安全是相互矛盾的。随着资源共享的进一步加强，随之而来的网络安全和信息安全问题也日益突出。因此，计算机网络的管理和维护，首先是网络安全的管理和维护，这也是网络管理员的首要职责。

5.2.1 网络安全概述

计算机网络的广泛应用已经对经济、文化、教育与科学和发展产生了重要的影响，同时也不可避免地带来了一些新的社会、道德、政治与法律问题。

从本质上来讲，网络安全就是网络上的信息安全，是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续、可靠、正常地运行，网络服务不中断。从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

国际标准化组织（ISO）引用 ISO 74982 文献中对安全的定义是：“安全就是最大程度地减少数据和资源被攻击的可能性”。Internet 的最大特点就是开放性，对于安全来说，这又是它致命的弱点。

网络安全涉及的内容既有技术方面的问题，也有管理方面的问题，两方面相互补充，缺一不可。技术方面主要侧重于如何防范外部非法攻击，管理方面则侧重于内部人为因素的管理。如何更有效地保护重要的信息数据，提高计算机网络系统的安全性，已经成为所有计算机网络应用必须考虑和解决的一个重要问题。

5.2.2 网络安全关注的范围

网络安全是网络必须面对的一个实际问题，同时网络安全又是一个综合性的技术。网络安全关注的范围如下。

（1）保护网络物理线路不会轻易遭受攻击。物理安全策略的目的是保护计算机系统、网络服务器、打印机等硬件实体和链路免受自然灾害、人为破坏和搭线攻击，确保计算机系统有一个良好的电磁兼容工作环境；建立完备的安全管理制度，防止非法进入计算机控制室和各种偷窥、破坏活动的发生。

（2）有效识别合法的和非法的用户。验证用户的身份和使用权限，防止用户越权操作。

（3）实现有效的访问控制。访问控制策略是网络安全防范和保护的主要策略，其目的是保证网络资源不被非法使用和非法访问。访问控制策略包括入网访问控制、操作权限控制策略和防火墙控制策略等方面的内容。

（4）保证内部的隐蔽性。通过 NAT 或 ASPF 技术保护网络的隐蔽性。

（5）有效的防伪手段，重要的数据重点保护。采用 IPSec 技术对传输数据加密。

（6）对网络设备、网络拓扑的安全管理。部署网管软件对全网设备进行监控。

（7）病毒防范。加强对网络中病毒的实时防御。

（8）提高安全防范意识。制定信息安全管理制度，赏罚分明，提高全员安全防范意识。

5.2.3 网络安全的目标

网络安全到底要保护什么？唯一的答案是：用户业务的安全。离开用户的业务谈安全是没有意义的。目前网络安全市场上常见的安全产品有防火墙、入侵检测系统、安全评估分析工具、防毒软件等，虽然这些产品由不同的厂商分别提供，但对于用户而言，它们缺一不可。

网络安全的目标应当满足以下几点。

（1）身份真实性：能对通信实体身份的真实性进行鉴别。

（2）信息机密性：保证机密信息不会泄露给非授权的人或实体。

（3）信息完整性：保证数据的一致性，能够防止数据被非受权用户或实体建立、修改和破坏。

（4）服务可用性：保证合法用户对信息和资源的使用不会被不正当地拒绝。

（5）不可否认性：建立有效的责任机制，防止实体否认其行为。

（6）系统可控性：能够控制使用资源的人或实体的使用方式。

（7）系统易用性：在满足安全要求的条件下，系统应当操作简单，维护方便。

（8）可审查性：对出现的网络安全问题提供调查的依据和手段。

网络安全的唯一真正目标是通过技术手段保证信息的安全。

5.2.4 网络安全防范体系

全方位的、整体的网络安全防范体系是分层次的，不同层次反映了不同的安全问题，根据网络的应用现状情况和网络的结构，可将安全防范体系分为物理层安全、系统层安全、网络层安全、应用层安全和管理层安全 5 个层次。

1．物理层安全

物理层的安全包括通信线路的安全、物理设备的安全和机房的安全等。物理层的安全主要体现在通信线路的可靠性、软硬件设备的安全性、设备的备份、防灾害能力、防干扰能力、设备的运行环境和不间断电源的保障等。

2．系统层安全

系统层的安全问题来自网络内使用的操作系统的安全，主要表现在 3 个方面：一是操作系统本身的缺陷所带来的不安全因素，主要包括身份认证、访问控制和系统漏洞等；二是对操作系统的安全配置问题；三是病毒对操作系统的威胁。

3．网络层安全

网络层的安全问题包括网络层身份认证、网络资源的访问控制、数据传输的保密与完整性、远程接入的安全、域名系统的安全、路由系统的安全、入侵检测的手段和网络设施防毒等。

4．应用层安全

应用层的安全问题主要由提供服务所采用的应用软件和数据的安全性产生，主要包括 Web 服务、电子邮件系统和 DNS 等，此外，还包括病毒对系统的威胁。

5．管理层安全

管理层的安全包括安全技术和设备管理、安全管理制度、部门与人员的组织规则等。管理的制度化在很大程度上影响着整个网络的安全，严格的安全管理制度、明确的部门安全职责划分、合理的人员角色配置都可以在很大程度上降低其他层次的安全漏洞。

5.2.5 网络中存在的威胁

1．黑客攻击

谈到网络安全，很容易联想到网络中的黑客。黑客的名词来自于英文 hacker 的发音，也被翻译为骇客。现在对黑客这个名词的普遍解释是：具有一定计算机和硬件方面的知识，通过各种技术手段，对计算机和网络系统的安全构成威胁的人或组织。

最早期的黑客行为是电话入侵技术，在电话普及初期，昂贵的电话费用不是一般人能承受的，于是，一些对电话技术了解颇多的人发明了一些电子装置，得以免费打电话。

随着计算机系统的产生和发展，一些专业技术人员开始深入探索系统上存在着的种种漏洞，尝试用自己的方式修补这些漏洞，并公开自己的发现。在早期，这些被称为黑客的人，他们热衷于解决难题，钻研技术，并乐于同他人共享成功。他们寻找网络漏洞，入侵主机，纯粹是技术上的尝试，绝不会进行资料窃取和破坏。这些黑客主要为了追求自己技术上的精进，对计算机全身心投入，为计算机技术的发展作出了很大的贡献，我们现在使用的很多软、硬件技术都是黑客发明的，很多早期的黑客后来成为 IT 界呼风唤雨的风云人物。

但是，随着网络的普及，黑客技术不断发展，队伍不断壮大，黑客的组成和社会内涵发生了巨大的变化，有些黑客开始尝试用自己的技术获取限制访问的信息，更有甚者怀着私利闯入远程主机，篡改和破坏重要数据，从此，黑客渐渐成为入侵者、破坏者的代名词。

很多人认为，黑客是技术高超的神秘人物，离自己很遥远，自己或者公司的网络系统

中没有什么值得获取或破坏的信息，不必担心他们的攻击，这种想法在多年以前可能没错。但随着网络上黑客技术文档和黑客工具的泛滥，只要愿意，没有计算机网络基础的外行也能很熟练地运用这些工具，成为一个可怕的入侵者。他们可能是你的同学、同事或邻居，他们想做的正是就近找一个目标进行实验，而用户很可能不幸成为他们的目标。这些黑客好比拿着原子弹的小孩，具有极大的攻击性，他们的攻击往往没有特定的目标，也不需要什么理由，入侵对他们来说只是一种恶作剧。还有一些黑客是怀着不良目的，借此获利的人，他们疯狂地入侵任何可能入侵的系统，寻找可能获得的任何利益，他们窃取有价值的资料对资料的主人进行敲诈、窃取各种有价值的网络账号、意图获取信用卡账号和口令，这些人对我们的威胁极大。

常见的黑客攻击行为有入侵系统、篡改网站、设置后门（以便以后随时侵入）、设置逻辑炸弹和木马、窃取和破坏资料、窃取账号、进行网络窃听、进行地址欺骗、进行服务攻击造成服务器瘫痪等。

2．病毒

计算机病毒是指那些具有自我复制能力的特殊计算机程序，它能影响计算机软、硬件的正常运行，破坏数据的正确与完整，影响网络的正常运行。病毒常常是附着于正常程序或文件中的一小段代码，随着宿主程序在计算机之间的复制不断传播，并在传播途中感染计算机上所有符合条件的文件。

计算机病毒也是程序，程序要发挥作用必须要运行，病毒要获得复制自身、感染其他文件并最后发作的能力，首先要将自身激活，并驻留内存，这个过程称为病毒的引导。不同类型的病毒，其引导方式各不相同，早期，有些病毒将自身隐藏于磁盘的主引导扇区（MBR）中，既能躲避病毒查杀程序的搜索，又能在系统启动时自动加载。大部分病毒隐藏在可执行文件中，只要可执行文件一运行，病毒就得以引导。也有病毒是隐藏在文档和媒体文件中的，如宏病毒，隐藏在具有宏功能的文档中，在宏被执行时，病毒也被激活。在 Windows 操作系统流行后，很多病毒隐藏在 Windows 系统文件中，随 Windows 系统启动而引导，由于 Windows 系统文件在系统运行过程中无法改写和删除，此类病毒很难被查杀。

病毒由一个载体传播到另一个载体，由一个系统进入另一个系统的过程称为传染。不同类型的病毒，其传染方式各不相同。早期，文件病毒通过驻留内存，截获对磁盘的调用命令，如列目录、运行文件、创建文件，然后通过更改指令将自身的副本悄悄写入磁盘上特定类型的文件中，当这些文件在计算机之间进行复制时，病毒也随之感染途经的所有未设防的计算机。

大部分病毒平时潜于系统中，不将自己暴露出来，只是不断复制自身，感染更多的计算机。当特定的条件满足时，病毒会被触发，称为病毒的发作。病毒发作的条件很多，如特定的日期，最有名的黑色星期五病毒，在每月 13 日又恰好是星期五的时候便会发作，还有 CIH 病毒，选择了每年的 4 月 26 日发作。还有病毒的触发条件是特定程序的运行、特定击键次数、特定的硬件设备等。

病毒发作的情况各不相同，有些病毒只是在屏幕上显示特定的图像和文字，然后就消失了，没有太大的破坏作用。而有些病毒则会造成系统死机，或是破坏和删除磁盘上的文件，甚至破坏磁盘分区表，使得整个计算机系统崩溃，在某些条件下，病毒甚至可以破坏

计算机硬件，如 CIH 病毒能破坏部分主板的 BIOS 芯片数据，使得计算机无法正常启动。

3．蠕虫

蠕虫（Worm）可以说是一类特殊的病毒，蠕虫通过分布式网络来进行扩散，与病毒类似，蠕虫也在计算机与计算机之间自我复制，但蠕虫可自动完成复制过程，而不需要通过文件作为载体复制，因为蠕虫能够接管计算机系统中传输文件或信息的功能。一旦计算机感染蠕虫，蠕虫即可独自传播。但最危险的是，蠕虫可大范围复制。例如，蠕虫可向电子邮件地址簿中的所有联系人发送自己的副本，联系人的计算机也将执行同样的操作，结果造成多米诺效应（网络通信负担沉重），业务网络和整个 Internet 的速度都将受到影响。一旦新的蠕虫被释放，传播速度将非常迅速，在极短的时间内就能造成网络堵塞。

蠕虫是一种通过网络传播的恶性病毒，它具有病毒的一些共性，如传播性、隐蔽性、破坏性等，同时具有自己的一些特征，如不利用文件寄生（有的只存在于内存中），以及与部分黑客技术相结合等。表 5-1 是蠕虫与普通病毒的主要区别。

表 5-1　蠕虫与普通病毒的主要区别

病毒	普通病毒	蠕虫
存在形式	寄存文件	独立程序
传染机制	宿主程序运行	主动攻击
传染目标	本地文件	网络计算机

蠕虫可以通过已知的操作系统后门主动攻击一台主机，然后设法感染这台主机并使其成为一个新的攻击源，去攻击其他主机。通过这种模式，网络上所有未设防的主机都将很快感染蠕虫，要想清除它们却很麻烦，只要网络中仍存在一台主机被感染，病毒就很可能会卷土重来。

通常来说，蠕虫不会破坏本地磁盘文件，但它的破坏能力却由于其强大的传播能力而远在普通病毒之上。例如，1999 年流行的“美丽杀手”蠕虫，使一些政府部门和大公司紧急关闭了网络服务器，经济损失超过 12 亿美元。2000 年开始流行的“爱虫”直至今日还有变种不时出现，造成的各项经济损失已超过 100 亿美元。2001 年开始流行的“求职信”病毒，造成全世界大部分邮件服务器无法正常运行，大量用户无法使用电子邮件系统，损失巨大。2003 年流行的“SQL 蠕虫王”病毒，在几小时之内造成大量金融数据库服务器崩溃，银行系统大面积瘫痪、自动提款机动作中断，直接经济损失超过 26 亿美元。

蠕虫已经成为网络中最大的威胁之一，是网络安全防护工作的重点。

4．木马

同希腊故事中的“特洛伊木马”类似，计算机中的木马是一些表面有用，实际目的是危害计算机安全性并破坏计算机系统的程序。早期的木马是黑客们特意编写后放置在他们制作的工具软件中，以随时获知这些工具的使用情况，现在很多人将自己编写的木马放置在其他应用程序中，使下载并使用这些程序的主机在不知不觉中感染木马程序。

完整的木马程序一般由两个部分组成：一个是被控制端（服务器）程序，另一个是控制端（客户端）程序。主机被感染即不知不觉中被安装了木马的服务器程序，如果主机被

安装了服务器程序，拥有控制端程序的人就可以通过网络控制用户的计算机，这时用户计算机上的各种文件、程序，以及在用户计算机上使用的账号、密码就无安全可言了。

木马的通常目的是窃取信息（如网络账号、信用卡密码、重要文档等）、监视和控制被感染主机。感染木马的计算机会偷偷通过网络向指定主机发送本机机密数据，或是莫名其妙地自动重启、自动关机，甚至出现主机被远程控制的情况。木马还常常同黑客技术相结合，如有些木马能够操纵被感染主机进行 ARP 欺骗与网络窃听（Sniffer），一台主机感染，整个网络安全性将遭受到威胁。

木马比病毒更隐蔽，更难以排查和清除，如不加以重视会给企业和个人造成不可估量的损失。

5．流氓软件

流氓软件是对利用网络进行散播的一类恶意软件的统称，这些软件或在不知不觉中偷偷安装在用户的系统中，或采用某种手段强行进行安装，或随某种软件一起安装到用户的系统中。

流氓软件一般以牟利为目的，强行更改用户计算机软件设置，如浏览器选项、软件自动启动选项、安全选项等。流氓软件常常在用户浏览网页过程中不断弹出广告页面，影响用户正常上网。流氓软件常常未经用户许可，秘密收集用户个人信息和隐私，有侵害用户信息和财产安全的潜在因素或者隐患。

流氓软件常抵制卸载，即使当时卸载成功，过一段时间系统中残留的程序又会偷偷地自动安装，使得用户不胜其烦。

流氓软件一般由正规企业或组织制作，具备部分病毒和黑客特征，但同病毒、木马不同，不会进行主动破坏和信息窃取，属于正常软件和病毒之间的灰色地带，因此大部分病毒和木马查杀程序不会检测和清除流氓软件。

5.2.6　网络安全防范技术

现在网络上攻击手段多种多样，用户的计算机系统有可能被病毒或木马感染，或者受到网络攻击和欺骗，造成主机无法正常访问网络。能够尽早了解主机和网络遭受攻击的类型，对解决网络安全问题有很大帮助。

现代网络操作系统都随系统提供了大量网络管理工具（命令），如通信测试命令：ping、tracert、pathping 等。利用这些工具可以方便、快捷地了解系统与网络的工作状态，甚至能解决一些网络攻击所造成的影响。

下面介绍如何利用 Windows 2000/XP/2003 中自带的工具来诊断和解决常见的网络安全问题。

1．网络连接故障诊断命令——ping

使用 ping 可以测试计算机名和计算机的 IP 地址，验证与远程计算机的连接，通过将 ICMP 回显数据包发送到计算机并监听回显回复数据包来验证与一台或多台远程计算机的连接，该命令只有在安装了 TCP/IP 协议后才可以使用。现在在 Windows 系统下执行“开始”

→“运行”命令，在打开的“运行”对话框中输入 cmd.exe 命令，按【Enter】键，下面介绍一下该命令：

ping [-t][-a] [-n count] [-r count] [-f][-i ttl][-v tos][[-j computer-list]|[-k computer-list]][-w timeout]destination-list

参数：

（1）-t：ping 指定的计算机直到中断。

（2）-a：将地址解析为计算机 NetBIOS 名。例如，c:\>ping –a 127.0.0.1，如图 5-2 所示。

Pinging localhost [127.0.0.1] with 32 bytes of data：（china-hacker 就是他的计算机名）

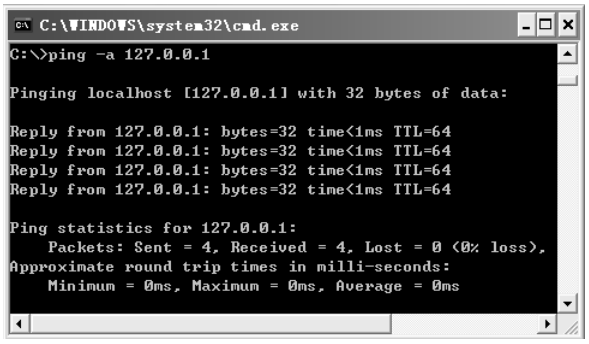


图 5-2　ping 命令查看计算机 NetBIOS 名

（3）-n count：发送 count 指定的 echo 数据包数，默认值为 4。

（4）-r count：在“记录路由”字段中记录传出和返回数据包的路由。通常情况下，发送的数据包是通过一系列路由才到达目标地址的，通过此参数可以设定探测经过路由的个数，限定能够跟踪 9 个路由，如图 5-3 所示。

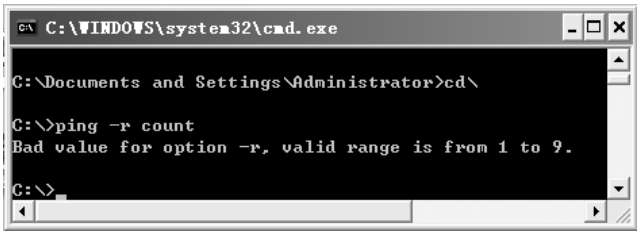


图 5-3　ping 命令查看数据包的路由

（5）-f：在数据包中发送“不要分段”标志。数据包就不会被路由上的网关分段。

（6）-i ttl：将“生存时间”字段设置为 ttl 指定的值。

（7）-v tos：将“服务类型”字段设置为 tos 指定的值。

（8）-j computer-list：利用 computer-list 指定的计算机列表路由数据包。连续计算机可以被中间网关分隔（路由稀疏源），IP 允许的最大数量为 9。

（9）-k computer-list：利用 computer-list 指定的计算机列表路由数据包。连续计算机不能被中间网关分隔（路由严格源），IP 允许的最大数量为 9。

（10）-w timeout：指定超时间隔，单位为毫秒（ms）。

（11）destination-list：指定要 ping 的远程计算机。

2．网络状态查看——netstat

netstat 是 Windows 操作系统提供用于查看与 IP、TCP、UDP 和 ICMP 协议相关的统计数据的网络工具，能检验本机各端口的网络连接情况。一般通过 netstat 来检查各类协议统计数据及当前端口使用情况，这些情况对检查和处理计算机是否存在网络安全隐患有很大的帮助。

netstat 命令支持的参数很多，比较常用的有以下几个参数。

（1）“-s”参数用来显示 IP、TCP、UDP 和 ICMP 的协议统计数据，经常与“-p”命令组合来查看指定协议的统计数据，当发现浏览器打开页面速度很慢，甚至根本无法打开页面或是电子邮件软件无法收发邮件时，很可能是 TCP 连接的问题，通过命令“netstat –s –p tcp”可以查看 TCP 协议统计数据，判断问题所在，如图 5-4 所示。

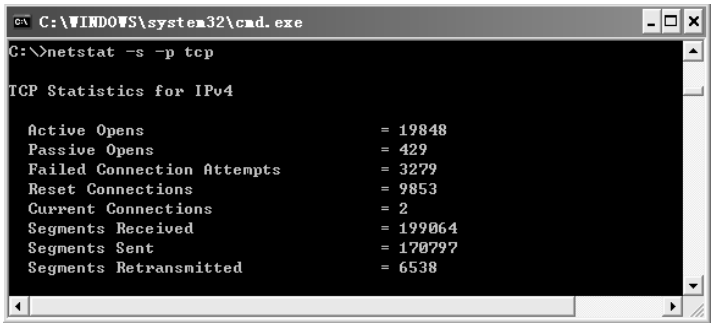


图 5-4　netstat 命令查看 TCP 协议统计数据

命令显示结果中各项参数的说明如下：

Active Opens	主动发起的 TCP 连接
Passive Opens	由对方发起的 TCP 连接
Failed Connection Attempts	失败的 TCP 尝试
Reset Connections	被复位的 TCP 连接
Current Connections	当前保持的 TCP 连接
Segments Received	接收到的数据段
Segments Sent	发送的数据段
Segments Retransmitted	重传处理的数据段

通过这些信息能够方便地了解问题是否出在连接上。例如，当前保持的 TCP 连接为 0，表示现在没有成功的 TCP 连接。如果重传处理的数据段数字非常大，则很可能是对端的网络连接通信质量有问题。

（2）“-e”参数用来看关于以太网的统计数据，如图 5-5 所示。它列出的项目包括传送的数据包的总字节数、错误数、数据报的数量和广播的数量。

如果使用“netstat -e”命令发现大量接收错误，则可能是网络整体拥塞、主机过载或本地物理连接故障；如果发现大量发送错误，则可能是本地网络拥塞或本地物理连接故障；如果发现广播数量过大，那么很可能网络正遭受广播风暴的侵袭。

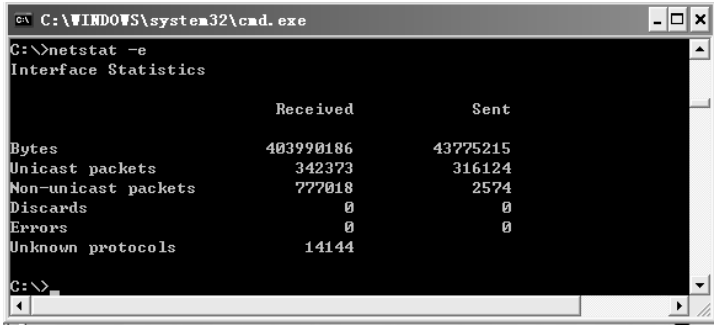


图 5-5　netstat 命令查看以太网统计数据

（3）“-a”与“-n”这两个参数进程一起使用，用来查看 TCP 与 UCP 连接情况，其中，“-a”参数用来显示所有连接及处于监听状态的端口，而“-n”参数则使用数字来表示主机与端口，更利于分析。

使用这个命令可以了解当前 TCP 与 UDP 连接情况，分析是否有不正常的网络连接及本地是否打开了某些不应打开的可疑端口，如图 5-6 所示。通常在感染了病毒或木马后，系统会打开特殊端口，用 netstat 可以很方便地确定系统是否被感染以及感染了哪种类型的病毒或木马，以便进行清除。

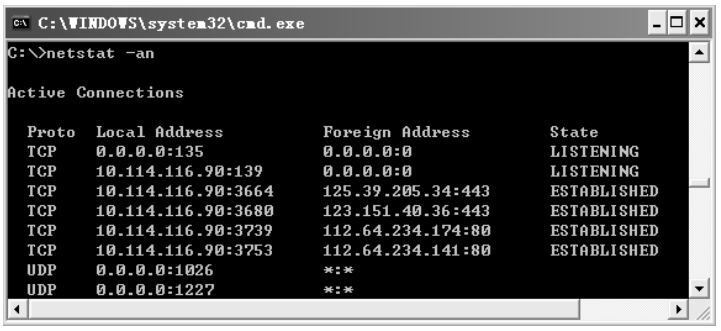


图 5-6　netstat 命令查看 TCP/UDP 连接情况

“netstat -an”命令显示的结果分为 4 列，其显示的信息说明如表 5-2 所示。

表 5-2　netstat -an 命令显示信息说明

列　名	名　称	说　明
Proto	协议类型	有两种协议，为 TCP 与 UDP
Local Address	本地地址端口	格式为：IP 地址:端口号
Foreign Address	对端地址端口	格式为：IP 地址:端口号
State	LISTEN ING	处于监听状态，等待其他主机发起对本 TCP 端口的连接请求
	SYN_SENT	处于连接尝试状态，已发送连接请求正等待回应
	SYN_RECEIVED	接收到其他主机的连接请求
	ESTABLISHED	连接已经建立，正进行正常的数据传输
	FIN_WAIT_1	端口已关闭，连接关闭中

续表

列　名	名　称	说　明
State	FIN_WAIT_2	连接已关闭，等待对方发送结束信号
	CLOSE_WAIT	对方已经关闭，等待端口关闭
	CLOSING	两侧端口都已经关闭，但数据仍未传送结束
	LAST_ACK	端口已经关闭，等待最后的确认信号
	TIME_WAIT	端口已经中断，正等待接收完所有仍在网络上的数据
	CLOSED	端口已经关闭

例如：

Proto	Local Address	Foreign Address	State
TCP	10.114.116.90:3753	112.64.234.141:80	ESTABLISHED

从这一行可以看出这是一个 TCP 连接，远端服务器 IP 地址是 112.64.234.141，端口号为 80，是 HTTP 服务器默认端口，本地 IP 地址是 10.114.116.90，端口为 3753，连接状态是“ESTABLISHED”正保持连接，属于正常通信状态，最后可以判断这个连接是本地主机正在访问 IP 地址为 112.64.234.141 的服务器的 WWW 服务。

更多时候，利用这个命令查看本地主机上是否打开了一些不应打开的可疑端口，特别是某些流行的木马的固定端口。例如，BO（Back Orifice）2000 使用 54320 端口、冰河使用 7626 端口，如果这些端口被打开，很可能已经被对应的木马入侵，需要进行清除。

3．本地路由管理

在计算机内存中，也存在着路由表，而且从条目格式、工作原理到所发挥的作用都与路由器上的路由表很相似，区别主要在于路由器的路由表管理不同子网之间的转发；而主机上的路由表主要用来指示主机向外发送数据包时，不同目的地通过哪些指定接口发送。当然，如果一台主机拥有多个网络接口，且连接着不同的子网，主机上同时启动着 IP 路由转发，它就成为一台真正的路由器。

对于本地计算机进行路由管理，首先要了解本地计算机是否开启了 IP 路由转发功能。所谓 IP 路由转发，是指主机是否能充当路由器的身份在不同子网间转发数据包。除了用于担当路由器身份的主机、远程接入服务器、VPN 服务器、NAT 服务器等专门配置的服务器主机外，一般的计算机不应开启 IP 路由转发服务，否则很可能是感染了木马，结合着 ARP 欺骗和 IP 数据包转发进行网络监听操作。

检查计算机是否开启 IP 路由转发最简单的方法是使用“ipconfig/all”命令，查看命令显示结果中的“IP Routing Enabled”参考取值，如果为“No”表示路由转发没有开启，如果为“Yes”表示已经开启 IP 路由转发，需要检查是否有问题，如图 5-7 所示。

如果要查看完整本地路由表，使用“route print”命令，也可以使用“netstat -r”命令，显示的结果完全一样，显示信息如图 5-8 所示，分为三个部分，第一部分是本地网络接口信息，即网卡基本信息，其中包括网卡的 MAC 地址和名称；第二部分是处于激活（工作）状态的路由表，分为 5 列，分别是 Network Destination（目标网络）、Netmask（子网掩码）、Gateway（网关）、Interface（接口）和 Metric（度量）。目标网络与子网掩码共同描述了目标的网络地址信息，即目的地；网关表示到达目的地的下一站或本地出口地址；接口说明

发送到这个目标网络需要使用哪个网络接口（网卡）；度量描述了到达目的地开销，当到达目的地存在多条路由时，根据它来判断优选哪条路由。

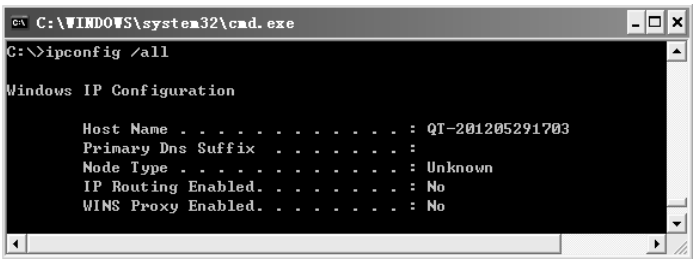


图 5-7　查看主机路由转发状态

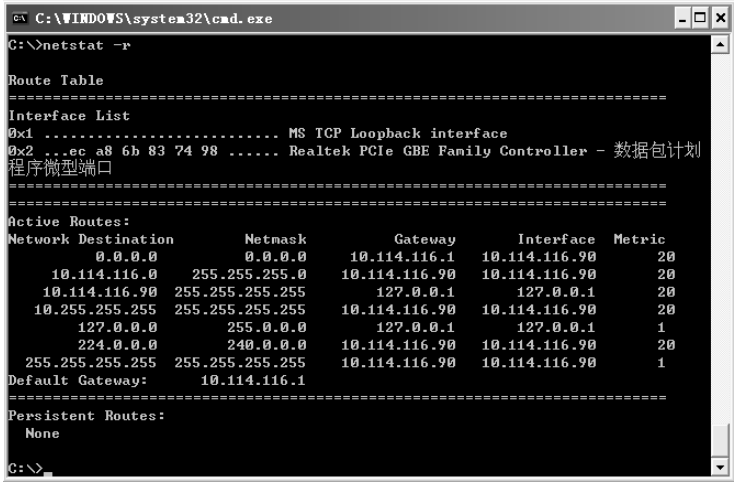


图 5-8　查看本地路由表

激活状态的路由表是当前正起作用的路由表，而静态路由表则是由管理员在计算机上定义并在每次开机时加载的路由条目。

通常，与路由相关的配置，只需要配置默认网关即可。检查网关是否配置正确，可以查看激活状态路由表的最后一行 Default Gateway 的配置信息。在激活状态路由表的最前面一行或几行，能看到目标网络与掩码都是 0.0.0.0 的路由条目，即网络号为 0.0.0.0 表示整个网络或任何 IP 地址，也描述了默认路由。

如果发生无法连接外网，但子网内通信正常的故障，很可能是默认网关的问题，应该先检查路由表，查看当前生效的默认网关有无发生变化或者丢失配置信息。

使用命令可增加、变更、删除路由表条目，增加路由条目使用命令“router add”、删除路由条目使用命令“router delete”、变更路由条目使用命令“router change”。

例如，在如图 5-8 所示的环境下，执行命令：

Route change 0.0.0.0 mask 0.0.0.0 10.114.116.254

将默认网关变更为 10.114.116.254

Route delete 0.0.0.0 mask 0.0.0.0

删除默认网关

Route add 0.0.0.0 mask 0.0.0.0 10.114.116.1

增加默认网关为：10.114.116.1

需要注意的是，这些通过命令增加或修改的路由条目在系统重新启动后不会保留，如果想让增加的路由条目在重新启动系统后仍发挥作用需要定义静态路由表，即在如图 5-6 所示界面显示的第三部分路由条目，定义静态路由使用命令“route print…-p”。

例如，执行命令：

Route add 10.114.116.0 mask 255.255.255.0 10.114.116.254 -p

增加静态路由条目，表示目标地址属于 10.114.116.0/24 网络的数据包将通过 10.114.116.254 进行转发而不是通过默认网关 10.114.116.1 进行转发。

Route delete 10.114.116.0 mask 255.255.255.0

删除以上定义的静态路由条目（删除静态路由条目不需要加-p 参数）

灵活地应用路由（route）命令，可以定位并解决很多由于路由表变化影响网络通信的故障，关于路由命令的更多参数可以参考微软提供的命令手册，或使用“route -?”命令查看联机帮助。

4．本地 ARP 缓存管理

在 TCP/IP 局域网通信过程中，广泛使用的是能体现网络结构、便于管理和理解的网络层地址——IP 地址，但我们已经了解，在网卡上固化的地址是物理地址——MAC 地址，网卡只能通过 MAC 地址来判断是否接收并处理网络上的数据帧，因此，在进行通信时，必须通过 ARP 协议将 IP 地址转换为 MAC 地址。

ARP 是一个在局域网通信中广泛使用的协议，使用广播包发送，网络中的每台主机都是 ARP 协议数据包的接收者和发送者。

由于计算机之间的通信频繁，如果每次通信都通过 ARP 协议来获取 MAC 地址信息会造成网络和主机资源的浪费，操作系统会在主机上建立一个本地 ARP 缓冲区（ARP Cache），在缓冲区中保存近期使用的 IP 地址与 MAC 地址映射记录。

当源主机需要将一个数据包发送到目的主机时，首先检查自己的 ARP 缓存中是否存在与该 IP 地址对应的 MAC 地址记录，如果有则直接将数据包发送到这个 MAC 地址，如果没有就向本地网段发起一个 ARP 请求的广播包，查询此目的主机对应的 MAC 地址。在这个 ARP 请求数据包里包括源主机的 IP 地址、MAC 地址，以及目的主机的 IP 地址。

网络中所有的主机收到这个 ARP 请求数据包后，会检查数据包中的目的 IP 地址是否与自己的 IP 地址一致。如果不同则忽略此数据包，如果相同则主机首先将发送端的 MAC 地址和 IP 地址添加到自己的 ARP 缓存中，如果 ARP 表中已经存在该 IP 地址信息则覆盖，然后给源主机发送一个 ARP 响应数据包，告诉对方自己的 MAC 地址。

源主机收到这个 ARP 响应数据包后，将得到的目的主机的 IP 地址和 MAC 地址添加到自己的 ARP 缓存中，并利用此信息开始数据的传输。如果源主机一直没有收到 ARP 响应数据包，表示 ARP 查询失败。

ARP 协议本身没有任何的验证机制，因此，接收到 ARP 包后，主机无法确认 ARP 协议数据包的发送者和信息是否属实。ARP 协议的工作方式产生了一个安全漏洞，别有用心的人可以轻易地冒名顶替发送 ARP 协议数据包，欺骗目标主机，并借此来窃取数据。

很多病毒、木马和黑客工具为了进行网络数据窃听，常常发送错误的 ARP 协议数据包来进行 MAC 地址欺骗，常被称为 ARP 欺骗和 ARP 缓存污染。ARP 欺骗会造成网络通信数据泄露，部分主机之间无法正常通信，甚至整个局域网无法访问外网，如 2006 年下半年开始流行的木马“传奇杀手”使得大量局域网无法访问 Internet，影响极大。

在 Windows 系列操作系统中，提供了管理本地 ARP 缓存的工具（arp），通过 arp 工具，可以检查本地 ARP 记录的正确性，并解决 ARP 欺骗造成的 ARP 缓存记录错误。

使用“arp -a”命令可以查看整个 ARP 缓存表，如图 5-9 所示。命令显示结果分为三列，分别是 Internet 地址（Internet Address，IP 地址）、物理地址（Physical Address，MAC 地址）及记录类型（Type）。记录类型分为动态记录（dynamic）和静态记录（static）两种，动态记录指通过 ARP 协议了解到的记录（如果一段时间不被刷新会自动删除），而静态记录指通过的记录（只要系统不重新启动就不会被清除）。

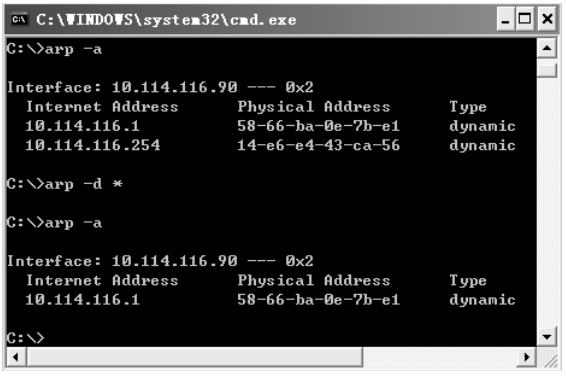


图 5-9　查看和清除 ARP 缓存记录

如果发现主机无法连接外网，但默认网关设置没有问题，网关工作也正常，那就要怀疑 ARP 记录是否正确了。检查“arp-a”命令显示的网关对应的记录是否存在，如果没有，可能是网关的故障，如果有网关记录，则需要比对其 MAC 地址（物理地址）是否真实。如果事先没有记录网关的正确 MAC 地址，也可以采用以下办法来判断：首先，使用“arp -d”命令删除本地所有 ARP 缓存记录；接着，使用 ping 命令测试与网关的连通性；最后，用“arp -a”命令查看并记录网关对应的 MAC 地址。这样做的依据是 ARP 欺骗主机必然是定时不断发送虚假的 ARP 数据包，这样先删除本地错误的记录，然后 ping 网关，主机会向网络发送 ARP 广播询问网关 MAC 地址，真正的网关会答复这个 ARP，这时查看记录即能获取正确的网关 MAC 地址。

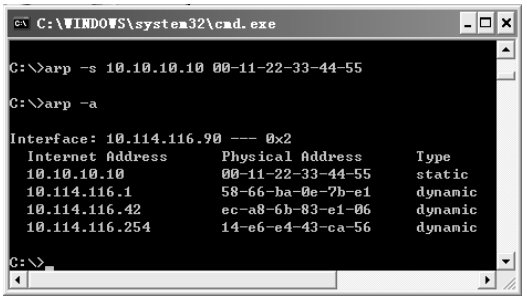


图 5-10　定义静态 ARP 缓存记录

如果发现确有 ARP 欺骗，可以利用 arp 工具定义静态 ARP 缓存记录，使本地主机暂时不受 ARP 欺骗的影响，命令格式是“arp –s ip 地址-MAC 地址”，如图 5-10 所示，定义了一条 IP 地址为 10.10.10.10、MAC 地址为 00-11-22-33-44-55 的静态记录，需要注意的是

静态记录重新启动系统后会清除，需要重新定义。

5.3　网络安全机制

1988 年国际标准化组织在有关安全结构的文件中指出，安全的意义是将资产及资源所受威胁的可能性降到最低程度。

随着 TCP/IP 协议群在互联网上的广泛采用，信息技术与网络技术得到了飞速发展。随之而来的是安全风险问题的急剧增加。为了保护国家公众信息网以及企业内联网和外联网信息和数据的安全，要大力发展基于信息网络的安全技术。

网络安全体系结构国际标准化组织（ISO）在开放系统互联参考模型（OSI/RM）的基础上，于 1989 年制定了在 OSI 环境下解决网络安全的规则：安全体系结构。它扩充了基本参考模型，加入了安全问题的各个方面，为开放系统的安全通信提供了一种概念性、功能性及一致性的途径。OSI 安全体系包含七个层次：物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。

5.3.1 加密技术

加密是保护数据免遭攻击的一种主要方法，它不但可用于维护数据的隐秘性，而且可用于协助辨识、数据完整性保护，以及各种其他安全防护工作。因此，加密机制是最重要的，也是用得最广泛的。

在计算机网络中，加密可分为“通信加密”（传输过程中的数据加密）和“文件加密”（存储数据的加密）。而通信加密又分为链路加密、节点加密和端－端加密三种方式。

1．节点加密

节点加密就是对相邻两个节点之间传输的数据进行加密。在这种方式中，加密仅对报文实施，而不对报头加密，以便于传输路由的选择。这种方式易被某种形式的报文分析所发觉，破坏者据此可获取与一个给定点收/发信息有关的统计资料。

2．链路加密

链路加密位于数据链路层，它对相邻节点之间的链路上所传输的数据进行加密，包括对数据和所有的报头都加密。这种方式能有效地抵抗线路串扰、主动或被动地搭线窃听所造成的威胁。

3．端-端加密

端-端加密是对用户之间传送的数据提供连续的保护。在初始节点上实施加密，在中间节点以密文形式传输，仅在目的节点才能解密。但加密时，报头仍为明码形式。这种方式对于防止线路串扰、搭线窃听、把网络中间节点数据转储到不同的主机是很有效的。同时对于实行故障修复和网络监控，以及防止复制网络软件和软件泄露等情况也十分有效。由

于加密位于表示层，虽然提供了灵活性，但却增加了主机的负担。

目前，在网络环境下经常使用的加密算法有对称性算法、非对称性算法和单向函数法。对称性算法是指加密和解密使用同一个密钥；非对称性算法是指加密和解密分别使用不同的密钥；单向函数法是指数据经由该函数转换后，所得结果与原数据不同，且从该结果数据难以推算还原至原来的数据。单向函数法虽然只能进行单向的转换，但在安全防护上有特殊的用途。

5.3.2 安全认证技术

网络安全认证技术是网络安全技术的重要组成部分之一。认证指的是证实被认证对象是否属实和是否有效的一个过程。其基本思想是通过验证被认证对象的属性来达到确认被认证对象是否真实有效的目的。被认证对象的属性可以是口令、数字签字，也可以是头像指纹、声音、视网膜这样的生理特征。认证常常被用于通信双方相互确认身份，以保证通信的安全，一般可分为两种：身份认证技术和消息认证技术。

1．身份认证技术

认证（Authentication）是证实实体身份的过程，是保证系统安全的重要措施之一。当服务器提供服务时，需要确认来访者的身份，访问者有时也需要确认服务提供者的身份。

身份认证是指计算机及网络系统确认操作者身份的过程。计算机网络系统是一个虚拟的数字世界。在这个数字世界中，一切信息包括用户的身份信息都是用一组特定的数据来表示的，计算机只能识别用户的数字身份，所有对用户的授权也是针对用户数字身份的授权。

2．消息认证技术

随着网络技术的发展，对网络传输过程中信息的保密性提出了更高的要求，这些要求主要包括以下几点。

（1）对敏感的文件进行加密，即使别人截取文件也无法得到其内容。

（2）保证数据的完整性，防止截获人在文件中加入其他信息。

（3）对数据和信息的来源进行验证，以确保发信人的身份。

消息认证实际上是对消息本身产生一个冗余的信息——MAC（消息认证码），消息认证码是利用密钥对要认证的消息产生新的数据块并对数据块加密生成的。它对于要保护信息来说是唯一的，因为可以有效地保护消息的完整性，以及实践发送方消息的不可抵赖和不能伪造。随着密码技术与计算机计算能力的提高，消息认证的实现方法也在不断的改进和更新之中，多种实现方式会为更安全的消息认证码提供保障。

5.4 防火墙技术

5.4.1 防火墙的概念

目前，保护网络安全最主要的手段之一是构筑防火墙。防火墙（Firewall）在计算机界

是指一种逻辑装置，用来保护内部的网络不受来自外界的侵害，是近年来日趋成熟的保护计算机网络安全的重要措施。防火墙是一种隔离控制技术，它的作用是在某个机构的网络和不安全的网络（如 Internet）之间设置屏障，阻止对信息资源的非法访问，防火墙也可以被用来阻止保密信息从企业的网络上被非法传出。

防火墙是在两个网络通信时执行的一种访问控制尺度，它能允许网络管理人员“同意”的人和数据进入他的网络，同时将网络管理人员“不同意”的人和数据拒之门外，阻止网络中的黑客来访问企业的网络，防止他们更改、复制或毁坏企业的重要信息。

5.4.2 防火墙的作用

防火墙的主要作用如下。

① 过滤信息，保护网络上的服务。通过过滤掉一些先天就不安全的服务，防火墙能够极大地增强内部网络的安全性，降低内部网络中主机被攻击的危险性。

② 控制对网络中系统的访问。防火墙具有控制访问网络中系统的能力。例如，来自外部网络的请求可以到达内部网络的指定机器，而无法到达内部网络的其他机器，保证了内部网络安全。

③ 集中和简化安全管理。使用防火墙可以使得网络管理无须针对内部网络的每台主机去专门配置安全策略，只需要针对防火墙做合理的配置，就可以实现对整个网络的保护。当安全策略需要调整时也只需修改防火墙即可，实现了对内部网络的集中和简化安全管理。

④ 方便监视网络的安全性。对一个内部网络而言，重要的问题并不是网络是否受到攻击，而是何时会受到攻击。防火墙可以在受到攻击时通过 E-mail、短信等方式及时通知网络管理员做出响应和处理。

⑤ 增强网络的保密性。所谓保密性，是指保证信息不会被泄露与扩散。保密性在一些网络中是首先要考虑的问题，因此通常被认为是无害的信息，实际上包含着对攻击者有用的线索。

⑥ 对网络存取和访问进行监控、审计。例如，防火墙会将内、外网络之间的数据访问加以记录，并提供关于网络使用的有价值的统计信息，供网络管理员分析。

⑦ 强化网络安全策略。防火墙提供了实现和加强网络安全策略的手段。实际上，防火墙向用户提供了对服务的访问控制方式，起到了强化网络对用户访问控制策略的作用。

当人们选择防火墙产品时，常常被说明材料上的参数搞得头晕眼花，下面对防火墙的技术参数做一个简单说明，以便今后能从参数了解防火墙的功能和性能。

（1）处理能力

① 防火墙最常见的用于描述处理能力的参数是并发会话/连接数。并发会话/连接数是指防火墙或代理服务器对其业务信息流的处理能力，是防火墙能够同时处理的点对点会话连接的最大数目，它反映防火墙对多个连接的访问控制能力和连接状态跟踪能力。这个参数的大小可以直接影响到防火墙所能支持的最大信息点数。

② 每秒新建会话/连接数是指在同一时间内防火墙能处理的新增会话的数目，从另一个方面反映了防火墙对连接的处理能力。

③ 吞吐量描述了单位时间通过防火墙的数据流量，以 bps 为单位，常见的商业产品吞吐量从几十兆到几百兆，甚至可达几千兆。在产品的吞吐量描述中，还常常将防火墙能支持的 VPN 吞吐量单独描述，VPN 吞吐量描述了防火墙对 VPN 数据的处理能力。

（2）接口类型和数量

防火墙接口决定了防火墙能提供的外网、内网的连接的类型和数目。防火墙的常见接口类型有以太网接口（10M Ethernet）、快速以太网接口（100M Ethernet）、千兆以太网接口（有 RJ-45 接口也有光纤接口或 GBIC 扩展口）。

防火墙的接口按连接网络类型分为外网口、内网口和 DMZ 接口，不同的接口有着不同的处理策略。有的防火墙还提供扩展接口用于用户自定义特殊的防护区域。

防火墙上提供了 Console 接口，主要用于初始化防火墙时，进行基本配置和系统维护操作，不同产品的 Console 接口类型可能不同，一般采用 RS-232 接口或 RJ-45 接口。有的防火墙还提供 PCMCIA 扩展插槽、IDS 镜像口、高可用性接口（HA）等，这些是根据防火墙的功能来决定的。

（3）功能

防火墙的功能决定了它是否能适应网络访问需求，是选择防火墙产品的一个重要指标，常见的功能参数有以下几个。

① 安全策略：安全策略是防火墙能对网络通信进行放行、拒绝、加密、认证、调试及监控的基础。安全策略能够支持的类型越多，策略的定义就越灵活，能够实现的防护功能也越强大。支持安全策略的数量也是防火墙的重要参数，策略的数量越多，防火墙支持的防护数量越多，但如果盲目提高策略数量，不能够与防火墙的处理能力相匹配，在策略应用太多后会造成防火墙性能急剧下降。

② 内容过滤：内容过滤是针对通信流量的内容进行过滤的功能，如阻止被标记为不安全的 URL、实行关键词检查、对 ActiveX 和恶意脚本进行过滤等。内容过滤提供针对当前 Internet 常见安全隐患非常有效的防御手段。

③ 用户认证：用户认证是针对内网用户的管理措施，要求内网用户必须经过认证，才能访问不可信网络（外网）。用户认证提供了对不同类型用户的分级管理，并能对用户访问外网的情况进行记录，以便出现安全问题后进行排查和审计。防火墙支持的用户认证方式有使用防火墙内建用户数据库、使用外部 Radius 数据库服务器、使用 IP/MAC 绑定等，可以根据具体需求进行选择。

④ 日志：防火墙能够对通过防火墙的请求、遭受到的攻击、配置修改等信息进行记录，日志分为安全日志、时间日志和传输日志等类型。防火墙支持的日志类型，记录的数量，是否支持存放到 Log 服务器进行分析审计，能否提供详细报表，是关系到今后网络管理工作的重要指标。

⑤ VPN 支持：主流防火墙都提供对虚拟个人网络 VPN 的支持，包括支持的 VPN 类型、最大 VPN 连接数、加密方式等参数。

此外，防火墙支持的管理界面、能否提供丰富的管理软件、系统更新的速度、本身的安全性等参数也是选择防火墙时需要注意的。

5.4.3 防火墙的分类及实现技术

1．防火墙的分类

防火墙的分类有多种方式。按照实现方式可分为软件防火墙和硬件防火墙。

（1）软件防火墙

软件防火墙以软件方式提供给客户，要求安装于特定的计算机和操作系统之上。安装完成后的计算机就成为防火墙，需要进行各项必要的配置，并部署于网络的恰当位置才能发挥其作用。

此处提到的软件防火墙与人们常常讲的个人防火墙并不完全相同。个人防火墙也是软件防火墙的一种，但它们安装于网络终端计算机上，只能提供对单机的安全防护，是一种功能比较单一的软件防火墙产品。

由于软件防火墙不在产品中提供计算机硬件，一般价格比较低廉，因此常常有人认为软件防火墙肯定不如硬件防火墙，这种观点是错误的，相对硬件防火墙，软件防火墙具有很多优点：软件防火墙安装配置灵活，易于使用；软件和硬件系统升级容易，升级成本低廉；功能配置灵活，有些产品还提供了二次开发的接口，可以根据用户的需求开发出特殊的功能。

常见的商业软件防火墙产品有以色列 Check Point 公司的 Firewall-1、微软公司的企业级网络安全解决方案 ISA（Microsoft Internet Security and Acceleration）等。

（2）硬件防火墙

硬件防火墙是以硬件形式提供给客户的，有些防火墙产品为了提高产品稳定性，常常定制了计算机硬件，这些计算机硬件与普通的 PC 没有本质区别，可能对体积和散热装置进行了改造，这类 PC 架构的硬件防火墙常常采用经过优化和裁减的 Linux 与 UNIX 操作系统，稳定性比较高。

这样的硬件防火墙与软件防火墙并无本质区别，只是提高了设备的稳定性、简化了系统的安装过程。

真正意义上的硬件防火墙也称为芯片级防火墙，它基于专门的硬件平台，不使用普通操作系统，将所有的防火墙功能都集成于特殊的 ASIC 芯片之中。借助专用的硬件支持，芯片级防火墙比其他种类的防火墙速度处理更快、处理能力更强、性能更高，由于芯片级防火墙的软、硬件都是为专业用途设计的，因此能提供更强大的功能和更简易的配置，稳定性和安全性也是所有产品中最高的，当然，芯片级防火墙的价格也是同级产品中最昂贵的。

2．防火墙的实现技术

根据防火墙的工作方式可分为包过滤型防火墙、代理服务型防火墙和状态监测防火墙。

（1）包过滤型防火墙

包过滤型防火墙也称为分组过滤型防火墙，这是一种通用型防火墙，因为这种防火墙不针对各个具体的网络服务采取特殊的处理方式；同时绝大多数防火墙均提供包过滤功能，且满足大多数的安全需求。

包过滤型防火墙工作于 ISO/OSI 模型的网络层与传输层。它根据分组包的源地址、目的地址、端口号、协议类型及标志，确定是否允许分组包通过。包过滤型防火墙所过滤的信息均位于数据包的 IP、TCP 或 UDP 包头。

包过滤型防火墙的特点如下。

① 有选择地允许数据分组穿过防火墙，实现内部主机和外部主机之间的数据交换。

② 作用于网络层和传输层。

③ 根据分组的源地址、目的地址、端口号、协议类型等确定是否让数据包通过。

④ 满足过滤条件的数据包才被转发，否则丢弃。

（2）代理服务型防火墙

代理服务型防火墙也称为应用网关防火墙，采用代理服务器（Proxy Server）的方式来保护内部网络。所谓代理服务，是指防火墙充当了内部网络与外部网络应用层通信的代理，内网主机与外网服务器建立的应用层链接实际上是先建立与代理服务器的链接，然后由代理服务器与外网主机建立应用层链接，这样便成功地实现了防火墙内、外计算机系统的隔离。

代理服务是设置在 Internet 防火墙网关上的应用，可以设定允许或拒绝特定的应用程序或者特定服务。例如，设定内部用户可以使用 E-mail 和 QQ 与外网联系，但不能使用 BT、电驴等 P2P 软件进行下载。代理服务型防火墙可以进行用户级访问控制，还能实施较强的数据流监控、过滤、记录和报告等功能。代理防火墙的另一个重要功能是高速缓存，缓存中存储着用户经常访问的站点内容，当另一个用户要访问同样的站点时，服务器就不用重复地去抓取重复的内容，直接从缓存中调取相应的数据，在提高用户访问速度的同时也节约了网络资源。

代理服务型防火墙解决了用户级访问控制的难题，能提供内部人员对外网的访问控制，还能对进、出防火墙的信息进行记录，便于监控和审计。代理服务型防火墙安装设置简单，可以采用软件方式提供，成本低廉。

代理服务型防火墙的主要不足之处在于所有跨网络访问都要通过代理来实现，牺牲了性能，如果在访问吞吐量大、连续数量多的情况下，代理将成为网络的瓶颈。使用代理服务型防火墙常常需要对客户主机进行相应的设定，而有些软件无法直接通过代理方式访问外网，必须安装第三方软件，牺牲了透明度，大大增加了网络管理的工作量。

代理服务型防火墙是中小企业进行网络安全防护与外网访问控制常用的解决方案，著名的代理服务型防火墙产品是美国 NAI 公司的 Gauntlet 防火墙，安装于 Linux 下的 Squid、Windows 下的 ISA、SyGate、WinGate 等软件也可实现代理服务型防火墙的功能。

（3）状态监测防火墙

状态监测技术结合了包过滤与代理技术的特点，具有最佳的安全特性。状态监测防火墙采用了一个网关上执行网络安全策略的软件引擎，称为检测模块。检测模块在不影响网络正常工作的前提下，采用抽取相关数据的方法对网络通信的各层实施监测，抽取的部分数据被称为状态信息。检测模块将获取的状态信息动态地保存起来作为今后制定安全决策的参考。检测模块支持多种协议和应用程序，并可以很容易地实现应用服务的扩充。与其他安全方案不同，当用户访问到达网关的操作系统前，状态监视器要抽取有关数据进行分析，结合网络配置和安全规定做出接纳、拒绝、鉴定或给该通信加密等决定。一旦某个访

问违反安全规定，安全报警器就会拒绝该访问，并记录下来向系统管理器报告网络状态。

状态监测防火墙能提供完整的网络安全防护策略、详细的统计报告，较快的处理速度，能够防御各种已知和未知网络攻击行为，适用于各类网络环境，在一些复杂的大型网络上更能发挥其优势，是当前主流防火墙技术。

状态监测防火墙的缺点是配置复杂，对系统性能要求较高，设备价格较高，对网络访问速度会造成影响。

状态监测技术由以色列 Check Point 公司首先提出，现在主流防火墙开发厂商的产品，如 Cisco 的 PIX 防火墙、NetScreen 防火墙等大都采用了状态监测技术。

5.4.4 防火墙的部署

虽然监测防火墙在安全上已超越了包过滤型和代理服务器型防火墙，但由于监测防火墙技术的实现成本较高，也不易管理，所以目前在使用中的防火墙产品仍然以第二代代理型产品为主，但在某些方面也已经开始使用监测防火墙。基于对系统成本与安全技术成本的综合考虑，用户可以选择性地使用某些监测技术。这样既能够保证网络系统的安全性需求，同时也能有效地控制安全系统的成本。

实际上，作为当前防火墙产品的主流趋势，大多数代理服务器（也称为应用网关）也集成了包过滤技术，这两种技术的混合应用显然比单独使用具有更大的优势。由于这种产品是基于应用的，应用网关能提供对协议的过滤。而且通过代理应用，应用网关能够有效地避免内部网络的信息外泄。正是由于应用网关的这些特点，使得应用过程中的矛盾主要集中在对多种网络应用协议的有效支持和对网络整体性能的影响上。

防火墙的部署：首先，安装防火墙的位置应该是公司内部网络与外部 Internet 的接口处，以阻挡来自外部网络的入侵；其次，如果公司内部网络规模较大，并且设置有虚拟局域网（VLAN），则应该在各个 VLAN 之间设置防火墙；再次，通过公网连接的总机构与各分支机构之间也应该设置防火墙，如果有条件，还应该同时将总机构与各分支机构组成虚拟专用网（VPN）。

安装防火墙的基本原则：只要有恶意侵入的可能、无论是内部网络还是与外部网络的连接处，都应该安装防火墙。

5.4.5 防火墙系统的局限性

防火墙系统存在以下局限性。

① 防火墙把外部网络当成不可信网络，主要是用来预防来自外部网络的攻击。它把内部网络当成可信任网络。然而事实证明，50%以上的黑客入侵来自于内部网络，但是防火墙对此却无能为力。这些可以把内部网分成多个子网，用内部路由器安装防火墙的方法以保护一些内部关键区域。这种方法维护成本和设备成本都会很高，同时也容易产生一些安全盲点，但毕竟比不对内部进行安全防范要好。

② 常常需要有特殊的、较为封闭的网络拓扑结构来支持，对网络安全功能的加强往往以网络服务的灵活性、多样性和开放性为代价。

③ 防火墙系统防范的对象是来自网络外部的攻击，而不能防范不经由防火墙的攻击。例如，通过 SLIP 或 PPP 的拨号攻击，绕过了防火墙系统而直接拨号进入内部网络。防火墙系统对这样的攻击很难防范。

④ 防火墙只允许来自外部网络的一些规则允许的服务通过，这样反而会抑制一些正常的信息通信，从某种意义上讲，大大削弱了 Internet 应用的功能，特别是对电子商务发展较快的今天，防火墙的作用很容易错失商机。

5.4.6 病毒、木马与流氓软件的防治

要做好对病毒、木马与流氓软件的防治，首先要保证系统本身的安全性，要为系统设置可靠的口令，定期为系统投入漏洞修复补丁，关闭不必要的端口和服务，这样能大大减小系统被攻击的概率。

1．病毒及其防治

计算机病毒具有的特点如下。

（1）破坏性

任何病毒只要侵入系统，都会对系统及应用程序产生不同程度的影响，凡是由软件手段能触及计算机资源的地方，均有可能受到计算机病毒的破坏。轻者会降低计算机工作效率，占用系统资源，重者可导致系统崩溃。

根据病毒对计算机系统造成破坏的程度，可以把病毒分为良性病毒与恶性病毒。良性病毒可能只是干扰显示屏幕，显示一些乱码或无聊的语句，或者根本没有任何破坏动作，只是占用系统资源。这类病毒较多，如 GENP、小球、W-BOOT 等。恶性病毒则有明确的目的，它们破坏数据、删除文件、加密磁盘甚至格式化磁盘，有的恶性病毒会对数据造成不可挽回的损失。这类病毒有 CHI、红色代码等。

（2）隐蔽性

病毒程序大多夹在正常程序之中，很难被发现，它们通常附在正常程序中或磁盘较隐蔽的地方（也有个别的以隐含文件形式出现），这样做的目的是不让用户发现它的存在。如果不经过代码分析，人们很难区别病毒程序与正常程序。一般在没有防护措施的情况下，计算机病毒程序取得系统控制权后，可以在很短的时间里传染大量程序，而且受到传染后，计算机系统通常仍能正常运行，用户不会感到有任何异常。

大部分病毒具有很高的程序设计技巧、代码短小精悍，其目的就是增加隐蔽性。病毒程序一般只有几百字节，而 PC 对文件的存/取速度可达每秒数十万字节以上，所以病毒程序在转瞬之间便可将这短短的几百字节附着到正常程序之中，不易被察觉。

（3）潜伏性

大部分计算机病毒感染系统之后不会马上发作，可长期隐藏在系统中，只有在满足特定条件时才启动其破坏模块。例如，PETER-2 病毒在每年的 2 月 27 日会提三个问题，答错后会将硬盘加密。著名的“黑色星期五”病毒在逢 13 号的星期五发作。当然，最令人难忘的是每年 4 月 26 日发作的 CHI 病毒。这些病毒在平时会隐藏得很好，只有在发作日才会显露出其破坏的本性。

（4）传染性

计算机病毒的传染性是指病毒具有把自身复制到其他程序中的特性。计算机病毒是一段人为编制的计算机程序代码，这段程序代码一旦进入计算机并得以执行，便会搜寻其他符合传染条件的程序或存储介质，确定目标后再将自身代码插入其中，达到自我繁殖的目的。只要一台计算机感染病毒，如不及时处理，那么病毒会在这台计算机上迅速扩散，其中的大量文件（一般是可执行文件）会被感染。而被感染的文件又成了新的传染源，传染源再与其他计算机进行数据交换或与网络接触，病毒便会在整个网络中继续传染。

正常的计算机程序一般是不会将自身的代码强行链接到其他程序之上的。而病毒却能使自身的代码强行传染到一切符合其传染条件的程序之上。是否具有传染性是判别一个程序是否为计算机病毒的最重要条件。

病毒防治，要以防为主，以查杀为辅，特别是 Windows 2000/XP/2003 操作系统，一旦感染病毒，很可能造成系统文件感染，清除病毒将会非常困难。

对付病毒，一般需使用专业的防病毒软件，市场上主流的防病毒软件有国外的卡巴斯基、F-SECURE、MACFEE、诺顿、趋势、熊猫、NOD32、AVG、F-PORT 等，国产软件有 KV 系列、金山毒霸、瑞星等。这些防病毒软件各有特点，在防、杀能力和效率上略有区别，但能力较强，但实时监控程序对系统资源占用较多，不太适合系统配置较低的主机。诺顿的实时监控占系统资源较少，速度也快，但可能会发生漏报现象，而且杀毒能力较弱，常常能查出病毒却无法清除。

对于杀毒软件，最重要的是要保证其实时监控随时处于打开状态，以及定时对杀毒软件的病毒特征库进行更新，只要能做到这两点，以上每一款杀毒程序都能保护用户的计算机系统不受病毒的侵袭。

相对于病毒的出现，防病毒软件的更新总是处于滞后状态，而且当前病毒的主要传播途径是网络，加速了病毒的传播速度，即使安装了杀毒程序且定时更新也有感染病毒的可能。如果感染了病毒也不用紧张，只要处置得当，大部分病毒都可以顺利清除。对于 Windows 操作系统，应该定期使用防病毒软件的查杀病毒功能对整个系统进行检查，对于被感染的文件，病毒查杀程序一般按照以下顺序进行处置：①清除病毒。将感染病毒后的文件复原，清除病毒，并保证文件不被破坏，清除病毒是人们最希望的处理结果。②转移并隔离病毒。将病毒进行隔离，保证病毒不会扩散和发作。对于暂时无法清除病毒的文件，将其保留于安全的隔离区，使病毒不会再对系统正常运行造成影响，等待以后做进一步处置，隔离病毒是针对一些无法清除病毒的临时性处理方式。③删除文件，对于一些感染病毒后源文件已经损坏且无法恢复的文件，病毒查杀程序会将其删除。

实际操作中，Windows 操作系统下感染的病毒常常是检查出有病毒，但杀毒程序既无法清除病毒，也无法隔离和删除病毒，这是因为 Windows 操作系统下很多系统文件在系统启动后是受保护的，杀毒程序无法更改这些文件。碰到这种情况，需要使用专门的病毒清除工具，各大厂商都会定期提供针对一种或多种病毒的清除工具，由于已经查到病毒，因此可以从防病毒软件的官方网站下载免费的针对性的病毒清除工具。在 Windows 下使用清除工具清除病毒需要在启动系统时按【F8】键进入安全模式，在安全模式下进行查杀，这是因为在安全模式下，很多不是必需的系统文件不会被加载和保护，以便于病毒清除工具进行处理。

有些情况下，查杀病毒后会造成系统启动故障，或是启动后有错误信息，这时不用急于重装系统，可以尝试使用系统安装光盘对系统进行修复，大部分启动故障都能通过这种方式解决。有些启动后的错误信息是由于病毒更改了系统启动信息，在系统启动时调用了病毒文件，而病毒文件已经被清除，造成错误，一般不影响正常使用，如果觉得每次开机有错误信息比较麻烦，可以通过启动管理程序（如微软的 msconfig、Windows 优化大师）对启动信息进行修改，如果对注册表比较熟悉，也可以直接更改注册表中的启动加载信息。

对于局域网上传播的蠕虫，查杀过程相对而言比较复杂，需要将所有主机从网络断开，并一一进行杀毒，保证所有主机均清除完成后方能将主机联入网络，否则，只要有一台主机没有清除干净，整个网络很快又会被蠕虫淹没。

2．木马及其防治

木马是一种在远程计算机之间建立起连接，使远程计算机能够通过网络控制本地计算机的程序，它的运行遵照 TCP/IP 协议，像间谍一样潜入用户的计算机，为其他人的攻击打开后门。

木马程序一般由两部分组成，分别是 Server（服务器）端程序和 Client（客户机）端程序。其中 Server 端程序安装在被控制计算机上，Client 端程序安装在控制计算机上，Server 端程序和 Client 端程序建立起连接就可以实现对远程计算机的控制。

首先，服务器端程序获得本地计算机的最高操作权限，当本地计算机接入网络后，客户机端程序可以与服务器端程序直接建立起连接，并可以向服务器端程序发送各种基本的操作请求，并由服务器程序完成这些请求，也就实现了对本地计算机的控制。

因为木马发挥作用必须要求服务器端程序和客户机端程序同时存在，所以必须要求本地机器感染服务器端程序，服务器端程序是可执行程序，可以直接传播，也可以隐含在其他的可执行程序中进行传播，但木马本身不具备繁殖性和自动感染的功能。

（1）木马的特征

据不完全统计，目前世界上有上千种木马程序。虽然这些程序使用不同的程序设计语言进行编制，在不同的环境下运行，发挥着不同的作用，但它们有着许多共同的特征。

① 隐蔽性。隐蔽性是木马的首要特征。木马类软件的 Server 端程序在运行时会使用各种手段隐藏自己。例如，大家所熟悉的修改注册表和 ini 文件，以便机器在下一次启动后仍能载入木马程序。通常情况下，采用简单地按【Ctrl+Alt+Delete】组合键的方法是不能看见木马进程的。

还有些木马可以自定义通信端口，这样就可以使木马更加隐蔽。木马还可以更改 Server 端的图标，让它看起来像个 ZIP 或图片文件，用户一不小心就会上当。

② 功能特殊性。通常，木马的功能都是十分特殊的，除了普通的文件操作以外，还有些木马具有搜索目标计算机中的口令、设置口令、记录用户事件、远程注册表的操作，以及颠倒屏幕、锁定鼠标等功能。

③ 自动运行性。木马程序通过修改系统配置文件或注册表的方式，在目标计算机系统启动时即自动运行或加载。

④ 欺骗性。木马程序要达到其长期隐蔽的目的，就必须借助系统中已有的文件，以防被用户发现。木马程序经常使用的是常见的文件名或扩展名，如“dll\win\sys\explorer 等字样”，或者仿制一些不易被人区别的文件名，如字母“l”与数字“1”、字母“o”与数字“0”。还有的木马程序为了隐藏自己，把自己设置成一个 ZIP 文件式图标，当用户一不小心打开它时，它就马上运行。木马编制者还在不断地研究、发掘新的欺骗手段，花样层出不穷，让人防不胜防。

⑤ 自动恢复性。现在，很多的木马程序中的功能模块已不再由单一的文件组成，而是具有多重备份，可以相互恢复。计算机一旦感染木马程序，想单独靠删除某个文件来清除，是不太可能的。

（2）木马的防治

大部分防病毒软件都提供了对木马程序的防治，只要打开防病毒程序的实时监控，木马一般无法进入系统，个人防火墙软件则是对付木马的另一可靠手段，安装个人防火墙，即使主机感染了木马，也不会因此丢失数据和泄露信息。此外，还有很多专门针对木马的防治工具，著名的国产木马防治软件——木马克星，对木马的防御和清除能力较强。

木马由于一般不感染其他文件，因此清除相对比较简单，但有些木马常常通过多种方式来启动木马程序，并将木马文件以不同的文件名存放于系统的不同位置，只要没有一次性清除所有文件，下次系统重启木马又将死灰复燃。清除木马最好采用专业病毒或木马查杀软件，如果要手工清除，则必须了解木马的所有痕迹，并一一进行清除。

3．流氓软件及其防治

流氓软件是介于病毒和正规软件之间的软件。计算机病毒是指自身具有或使其他程序具有破坏系统功能、危害用户数据或其他恶意行为的一类程序。这类程序往往影响计算机使用，并能够自我复制。正规软件是指为方便用户使用计算机工作、娱乐而开发，面向社会公开发布的软件。“流氓软件”介于两者之间，同时具备正常功能（下载、媒体播放等）和恶意行为（弹广告、开后门），给用户带来危害。

（1）流氓软件的分类

根据不同的特征和危害，困扰广大计算机用户的流氓软件主要有以下几类。

① 广告软件（Adware）。广告软件是指未经用户允许，下载并安装在用户计算机上或与其他软件捆绑，通过弹出式广告等形式牟取商业利益的程序。

危害：此类软件往往会强制安装并无法卸载；在后台收集用户信息牟利，危及用户隐私；频繁弹出广告，消耗系统资源，使其运行变慢等。

例如，用户安装了某下载软件后，会一直弹出带有广告内容的窗口，干扰正常使用。还有一些软件安装后，会在 IE 浏览器的工具栏位置添加与其功能不相干的广告图标，普通用户很难将其清除。

② 间谍软件（Spyware）。间谍软件是一种能够在用户不知情的情况下，在其计算机上安装后门，用于收集用户信息的软件。

危害：用户的隐私数据和重要信息会被“后门程序”捕获，并被发送给黑客、商业公司等。这些“后门程序”甚至能使用户的计算机被远程操控，组成庞大的“僵尸网络”，这是目前网络安全的重要隐患之一。

例如，某些软件会获取用户的软、硬件配置，并发送出去，用于商业目的。

③ 浏览器劫持。浏览器劫持是一种恶意程序，通过浏览器插件、BHO（浏览器辅助对象）、Winsock LSP 等形式对用户的浏览器进行篡改，使用户的浏览器配置不正常，被强行引导到商业网站。

危害：用户在浏览网站时会被强行引导到其指定的网站，严重影响正常上网。

例如，一些不良站点会频繁弹出安装窗口，迫使用户安装某浏览器插件，甚至根本不征求用户意见，利用系统漏洞在后台强制安装到用户计算机中。这种插件还采用了不规范的软件编写技术（此技术通常被病毒使用）来逃避用户卸载，往往会造成浏览器错误、系统异常重启等。

④ 行为记录软件（Track Ware）。行为记录软件是指未经用户许可，窃取并分析隐私数据，记录用户计算机使用习惯、网络浏览习惯等个人行为的软件。

危害：危及用户隐私，可能被黑客利用来进行网络诈骗。

例如，一些软件会在后台记录用户访问过的网络并加以分析，有的甚至会发送给专门的商业公司或机构，此类机构会据此窥测用户的爱好，并进行相应的广告推广或商业活动。

⑤ 恶意共享软件（Malicious Shareware）。恶意共享软件是指某些共享软件为了获取利益，采用诱骗、试用陷阱等方式强迫用户注册，或在软件体内捆绑各类恶意插件，未经允许即将其安装到用户计算机中。

危害：使用“试用陷阱”强迫用户进行注册，否则可能会丢失个人资料等数据。软件集成的插件可能会造成用户浏览器被劫持、隐私被窃取等。

例如，用户安装某款媒体播放软件后，会被强迫安装与播放功能毫不相干的软件（搜索插件、下载软件）而不给出明确提示；并且用户卸载播放器软件时，系统不会自动卸载这些附加安装的软件。

又如，某加密软件，试用期过后所有被加密的资料都会丢失，只有交费购买该软件才能找回丢失的数据。

（2）流氓软件的防治

流氓软件虽然大都提供了卸载选项，但很难真正从系统上卸载干净，常常是刚卸载，一旦连接网络又出现了。而且，防病毒软件一般无法对流氓软件进行阻止和清除。要防止流氓软件进入系统，首先要对自己上网和安装软件的习惯进行规范。流氓软件进入系统的一个途径是与其他软件捆绑安装，在安装过程中，会提示用户是否确认安装，只要仔细查看软件安装过程中对话框的内容，可以阻止很大一部分流氓软件；流氓软件进入系统的另一个途径是以浏览器插件形式安装，这种情况浏览器也会做出提示，只要注意，也完全可以避免。

如果系统上已经存在流氓软件，可以采用专门的流氓软件清除工具，或是手动进行清除。如果浏览器被劫持（被篡改了首页、安全选项、会自动弹出窗口，又无法恢复的情况），也可以使用 IE 恢复工具进行处理，比较著名的 IE 恢复工具是 HijackThis，它可以修复各种流氓软件、木马、病毒对浏览器选项的更改，并清除通过各种途径在系统启动中加载的非法程序。

习　题　5

一、填空题

1．网络管理中心，通常由一组功能不同的_____组成，它们指挥和_____网络中的其他设备一起完成网络管理的任务。

2．一个功能完善的网络管理系统，对网络的使用有着极为重要的意义。它通常具有_____、_____、_____、_____及安全管理等功能。

3．安全管理功能是用来保护_____的。

4．简单网络管理协议的体系结构是从早期的简单_____协议发展而来的，是 Internet 组织用来_____采用 TCP/IP 协议的互联网和以太网的。

5．SNMP 管理模型中有三个基本组成部分：_____、_____和_____。

6．根据网络故障对网络应用的影响程度，网络故障一般分为_____故障和_____故障两大类。

7．排除网络层故障的基本方法是沿着从源到目的地的路径查看_____上的路由表，同时检查那些路由器接口的_____地址是否正确。

8．故障排除常用方法有_____、_____、_____及_____。

9．网络安全就是网络上的_____安全，是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到_____、更改、_____，系统连续、可靠、正常地运行，网络服务不中断。

10．全方位的、整体的网络安全防范体系是分_____的，不同层次反映了不同的安全问题，根据网络的应用现状情况和网络的结构，可将安全防范体系分为_____安全、_____安全、_____安全、_____安全和_____安全 5 个层次。

11．计算机病毒是指那些具有_____能力的特殊计算机_____，它能影响计算机软、硬件的正常运行，破坏_____的正确与完整，影响网络的正常运行。

12．蠕虫是一种通过网络传播的_____病毒，它具有病毒的一些共性，如_____、_____、破坏性等，同时具有自己的一些特征，如不利用文件寄生（有的只存在于内存中），以及与部分黑客技术相结合等。

13．完整的木马程序一般由两个部分组成：一个是_____程序，另一个是_____程序。

14．网络中存在的威胁主要有_____、_____、_____、_____和_____。

15．OSI 安全体系包含七个层次：_____、_____、_____、_____、会话层、_____和_____。

16．在计算机网络中，加密可分为“_____”和“_____”。而通信加密又分为

_____加密、_____加密和_____加密三种方式。

17．防火墙的主要作用可分为_____、_____、_____、_____、_____、_____、_____。

18．防火墙的分类有多种方式。按照实现方式可分为_____防火墙和_____防火墙。根据防火墙的工作方式可分为_____防火墙、_____防火墙和_____防火墙。

19．计算机病毒具有的特点有_____、_____、_____、_____。

20．木马的主要特征有_____、_____、_____、_____、_____。

21．流氓软件主要分为_____、_____、_____、_____、_____。

22．病毒查杀程序一般按照以下顺序进行处置：_____、_____、_____。

二、简答题

1．SNMP 的目标提供了哪些管理操作？

2．连通性故障的表现形式有几种？

3．计算机出现网络性能故障的主要原因是什么？

4．在使用分层故障排除法进行故障排除时，具体每一层次的关注点有何不同？

5．网络安全关注的范围有哪些？

6．常见的黑客攻击行为有哪些？

7．防火墙的主要作用有哪些？

8．防火墙系统存在哪些局限性？

9．蠕虫与普通病毒的主要区别是什么？

10．网络状态查看工具 netstat 的主要参数有哪些？基本用途是什么？

11．什么是网络防火墙？其基本功能是什么？

12．根据防火墙的工作方式，防火墙可分为几类？简述各类防火墙的差别。

第6章 交换与路由技术

内容摘要

- 网络设备的基本配置
- 虚拟局域网（VLAN）及其配置
- 生成树协议、端口聚合及其配置
- 路由协议及其配置
- 访问控制列表（ACL）及其配置
- 网络地址转换（NAT）及其配置
- 层次化网络设计模型的特点

学习目标

- 掌握网络设备的基本配置
- 掌握虚拟局域网（VLAN）及其配置
- 理解生成树协议、端口聚合及其配置
- 掌握路由协议及其配置
- 掌握访问控制列表（ACL）及其配置
- 理解网络地址转换（NAT）及其配置
- 了解层次化网络设计模型

随着 Internet 的发展，交换与路由技术得到了广泛的推广和应用。数据交换技术也从最早简单的电路交换发展到二层交换，从二层交换又逐渐发展到今天较为成熟的三层交换，再发展到将来的高层交换。因此，在大型骨干网中，各种模块化、智能化、多功能的网络设备正扮演着重要的角色。

6.1 路由器和多层交换机概述

路由器（Router）是一种典型的网络层设备，负责在网络层间传输数据分组，并确定网络上数据传送的最佳路径，完成网络层间中继的任务。一般来说，异种网络互联与多个子网互联都需用路由器来完成。因此，路由器不仅具有寻址和转发的功能，可实现数据分组从一个网络到另一个网络的传输，还可以对网络、地址、协议、端口号、数据包进行过滤和筛选，实现对网络信息的安全保护。如图 6-1 所示，是几款模块化的路由器和模块接口卡，用户可以根据需求选用模块的类型和数量。

图 6-1　模块化的路由器和模块接口卡

交换机（Switch）是一种具有简化、低价、高性能和多端口密集特点的交换产品。根据 OSI 层次通常可分为二层交换机和三层交换机。通常所说的交换机就是指二层交换机（又称为 LAN 交换机），属于数据链路层设备，是二层交换技术在局域网中的典型应用。二层交换技术可以识别数据帧中的 MAC 地址信息，根据 MAC 地址转发数据帧，并将这些 MAC 地址与对应的端口，记录在自己内部的一个 MAC 地址表中。数据帧的发送与接收正是围绕这张 MAC 地址表，从而建立了一条临时的交换路径，使数据帧由源地址发送到目的地址。

随着网间互访的不断增加，单纯使用路由器来实现不同网间的访问，不但由于端口数量有限，而且路由速度较慢，从而限制了网络的规模和访问速度。基于这种情况，三层交换机便出现了。三层交换机是为 IP 设计的，既可以工作在协议第三层替代或部分完成传统路由器的功能，同时又具有几乎与第二层交换等同的速度，接口类型简单，且价格相对便宜些，非常适用于大型骨干网内的数据路由与交换。三层交换机与二层交换机工作方式类似，除了使用二层 MAC 地址进行交换外，还使用 OSI 网络标准参考模型中的第三层（网络层）实现了不同子网间数据包的 IP 高速路由转发。简单地说，三层交换技术就是：二层交换技术＋三层转发技术。因此，三层交换技术的出现，解决了局域网中网段划分之后，网段中子网必须依赖路由器进行管理的局面，解决了传统路由器低速、复杂所造成的网络瓶颈问题。

6.1.1 网络设置的配置方法

1．带外管理——利用控制台（Console）端口配置

对于新购进的网络设备（本章多指多层交换机和路由器）一般都有出厂默认设置，如果用户想知道其网络接口是否启用和参数如何，通常用一根配置线（反转线）将计算机的串行口（COM）和网络设备的控制台（Console）端口相连，通过使用计算机中 Windows 自带的“超级终端”对网络设备进行后续配置和管理。如图 6-2 所示为一款三层交换机及其硬件连接。

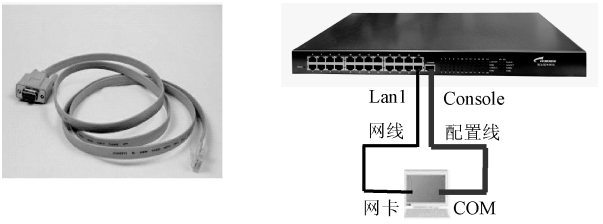


图 6-2　三层交换机及其硬件连接

具体配置步骤如下。

（1）执行“开始”→“所有程序”→“附件”→“通信”→“超级终端”命令。

（2）打开“超级终端”窗口，如果是首次使用超级终端会出现如图 6-3 所示的对话框。

（3）任意填入一个区号后，单击“确定”按钮，出现如图 6-4 所示的对话框。

图 6-3　“位置信息”对话框

图 6-4　“电话和调制解调器选项”对话框

（4）再次单击“确定”按钮，便打开如图 6-5 所示的对话框。

（5）名称任意填写，然后单击“确定”按钮，出现如图 6-6 所示的对话框。设置好后单击“确定”按钮。

（6）在“连接时使用”列表栏中选择当前计算机连接使用的 COM1 端口，然后单击“配置”按钮，出现如图 6-7 所示的对话框。

（7）按照如图 6-7 所示的参数进行设置或单击“还原为默认值”按钮，然后单击“确定”按钮，就会打开“超级终端”窗口自动连接网络设备，出现如图 6-8 所示的命令提示符配置窗口。

图 6-5　“连接描述”对话框

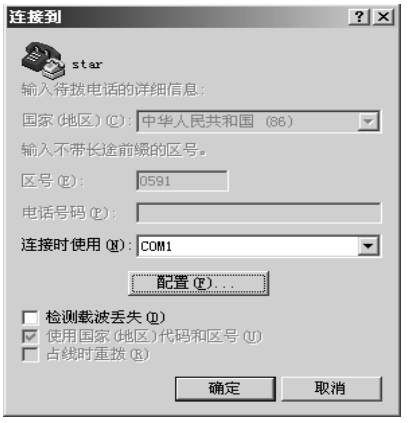


图 6-6　“连接到”对话框

图 6-7　端口设置

图 6-8　命令提示符配置窗口

说明：

（1）配置线（反转线）与网线不同，其线序既不是 T568A，也不是 T568B，而是两头的线序正好相反。

（2）利用配置线（反转线）通过控制台端口对网络设备配置，既不占用局域网的带宽，也不占用广域网的带宽，因此称为带外管理。

2．带内管理——利用 telnet 命令远程登录配置

用一根直连网线将 PC 的网卡接口（RJ-45）和网络设备的 LAN 端口相连，在 PC 中打开命令提示符窗口，在命令行中输入命令“telnet 网络设备管理 IP 地址”，输入远程登录密码，就可以进入网络设备的各命令配置模式。

说明：

（1）远程登录的计算机不是连接在网络设备 Console 端口上的 PC，而是接入网络中的任意一台 PC，是会占用网络带宽的，因此称为带内管理。

（2）远程登录方式不能用来配置新网络设备，新网络设备必须先用控制台（Console）端口配置其管理 IP 地址、远程登录密码和特权密码等参数。

6.1.2 网络设备的命令行操作

1．命令模式

网络设备（多层交换机和路由器）的所有命令是按模式分层的，每种模式中定义了一组命令，所以要想使用某个命令，必须先进入相应的模式。各种模式可通过命令提示符进行区分。

登录网络设备的命令提示符格式：提示符名 模式

（1）提示符名一般是设备的名字，交换机的默认名字为“Switch”，路由器的默认名字为“Router”。

（2）提示符模式表明了当前所处的操作模式。例如：“>”代表用户模式，是用户最先登录的模式；“#”代表特权模式。

表 6-1 所列的是常见的几种命令模式。

表 6-1　常见的命令模式

模　式	提 示 符	说　明
用户模式	Router>	可用于查看系统基本信息和进行基本测试
特权模式	Router#	查看、保存系统信息
全局配置模式	Router（config）#	配置设备的全局参数
接口配置模式	Router（config-if）#	配置设备的各种接口
线路配置模式	Router（config-line）#	配置控制台、远程登录等线路
路由配置模式	Router（config-router）#	配置路由协议
VLAN 配置模式	Switch（config-vlan）#	配置 VLAN 参数

2．命令模式的切换

网络设备的命令模式大体可分为四步：用户模式→特权模式→全局配置模式→其他配置模式。要进入某模式时，需要逐步进入，如表 6-2 所示。

表 6-2　命令模式的切换及说明

配 置 模 式	命 令 举 例	说　明
进入用户模式	Router>_	登录后就进入
进入特权模式	Router>enable Router#	在用户模式中输入 enable 命令

续表

配 置 模 式	命 令 举 例	说　明
进入全局配置模式	Router#configure terminal Router（config）#	在特权模式中输入 configure terminal 命令
进入接口配置模式	Router（config）#interface f0/1 Router（config-if）#	在全局配置模式中输入 interface 命令，后可带不同参数
进入线路配置模式	Router（config）#line console 0 Router（config-line）#	在全局配置模式中输入 line 命令，后可带不同参数
进入路由配置模式	Router（config）#router rip Router（config-router）#	在全局配置模式中输入 router 命令，后可带不同参数
进入 VLAN 配置模式	Switch（config）#vlan 10 Switch（config-vlan）#	在全局配置模式中输入 vlan 命令，后可带不同参数
退回到上一模式	Router（config-if）#exit Router（config）#	用 exit 命令可退回到上一模式
退回到特权模式	Router（config-if）#end Router#	输入 end 命令或按【Ctrl+Z】组合键可从各配置模式中直接退回到特权模式
退回到用户模式	Router#disable Router>	从特权模式退回到用户模式

3．命令行的编辑技巧

（1）命令不区分大小写。

（2）可以使用简写。

命令的每个单词只需要输入前几个字母。只要输入的前几个字母能够与其他命令相区分开即可。例如，configure terminal 命令可简写为 conf t。

（3）用【Tab】键可补全简化的命令。

如果想把简写的命令补全，可按【Tab】键补全完整的命令单词。例如，输入 conf（Tab）t（Tab）⇨ configure terminal。

（4）可以调出历史命令来简化命令的输入。

用【↑】键（【Ctrl+P】）和【↓】键（【Ctrl+N】）调出历史命令再按【Enter】键就可执行此命令。

（5）编辑快捷键：

【Ctrl+A】——光标移到行首，【Ctrl+E】——光标移到行尾，【Ctrl+F】——下移一个字符。

（6）用“?”可帮助输入命令和参数。

在提示符下输入“?”可查看该提示符下的所有命令，在命令后加“?”，可查看该命令后的所有参数，在该参数后再加“?”，可查看该参数后跟的所有参数，以此类推，直至遇到提示“<cr>”，说明命令结束。

4．常见命令行错误提示

（1）% Ambiguous command。

用户没有输入足够的字符，设备无法识别唯一的命令。

（2）% Incomplete command。

命令缺少必需的关键字或参数。

（3）% Invalid input detected at '^' marker。

符号 ^ 指明了输入错误命令单词的位置。

5．no 和 default 选项

（1）no 选项的用法是在命令前加 no 前缀，可用来禁止某个功能或者删除某项配置。例如，no shutdown，no ip address。

（2）default 选项的用法是在命令前加 default 前缀，用来将设置恢复为默认值。例如，default hostname。

6.1.3 网络设备的基本配置

1．配置主机名

在默认情况下，交换机的主机名通常为“Switch”，路由器的主机名通常为“Router”。当网络中存在多个网络设备时，为了网络管理员便于区分网络中的网络设备而特意为其定义的一个有意义的名称。可以在全局模式下通过“hostname”命令来实现，其配置命令如下：

```
Router（config）#hostname R1
/设置路由器的主机名为 R1
R1（config）#
```

2．口令设置

（1）控制台口令：利用配置线（反转线）通过控制台 console 端口对网络设备进行配置时，为了安全起见，通常为该端口的登录设置密码口令。配置命令如下：

```
Router（config）#line console 0
/进入控制台端口的 line 配置模式
Router（config-line）#password abc123
/设置本地登录密码为 abc123
Router（config-line）#login
```

（2）远程登录口令：通常网络设备支持多个虚拟终端， 一般为 16 个（0～15）。通过网络中的远程终端设备，利用“Telnet　IP address”命令远程登录网络设备时，需要输入该命令，才能进入网络设备配置的命令提示符。配置命令如下：

```
Router（config）#line vty 0 4
/对 0～4 条虚拟终端线路进行设置
Router（config-line）#password abc123
```

```
/设置远程登录密码为 abc123
Router（config-line）#login
/使密码生效
```

注意：远程登录口令是用 Telnet 登录的必备条件。

（3）特权口令：在网络设备配置的命令提示符为用户模式下，需要输入该口令，才能进入特权模式。

```
Router（config）#enable password abc123
/设置特权模式密码为 abc123
Router（config）#enable secret abc123
/设置特权模式密码为 abc123
```

两者的区别：

① enable password 命令配置的口令是以明文方式存储的，在 show running-config 命令中可见。

② enable secret 命令配置的口令是以密文方式存储的，在 show running-config 命令中不可见。

③ 以上两个口令只需配置一个，如果两个都配置了，则由用户模式进入特权模式，要用 enable secret 定义的口令。由此可见，enable secret 定义的口令优先级高于 enable password 定义的口令优先级。

3．文件的查看、保存与删除

（1）查看当前运行配置

网络设备当前运行的配置文件暂存于其内部的 RAM（随机存储内存）中，名为“running-config”。当网络设备断电或重新启动后，此文件丢失。查看当前的配置，可以在特权模式下通过“show”命令来实现，配置命令如下：

```
Router#show running-config
```

（2）查看启动配置

网络设备启动配置文件一般位于其内部的 NVRAM（非易失性随机存储器）中，名为“startup-config”。当设备启动时，它被装入 RAM，成为运行配置文件。查看启动配置，可以在特权模式下通过“show”命令来实现，配置命令如下：

```
Router#show startup-config
```

（3）保存当前配置

由于网络设备内部的 RAM（随机存储内存）中的当前运行配置文件“running-config”在断电或重新启动时会丢失，所以在配置好设备后，应该把 RAM 中当前的配置文件“running-config”保存到 NVRAM（非易失性随机存储器）中，为“startup-config”，这样以后就可以长久使用了。配置命令如下：

```
Router#copy running-config startup-config
或 Router#write
```

说明：write 与 copy running-config startup-config 这两条命令的功能相同。

（4）删除配置

```
Router#delete flash：config.text
```

说明：config.text 是配置文件在 NVRAM 中的文件名，它被删除后，再重新启动设备时就会自动进入网络设备出厂的默认配置。

4．端口配置

（1）端口的选择

网络设备的端口分为 Ethernet（10Mbps）、Fast Ethernet（10/100Mbps）、Gigabit Ethernet（10/100/1000Mbps）、Serial 几种类型。在实际配置时，网络设备端口的类型一定要写正确。一般可以先用“show”命令查看一下网络设备各端口的类型。

例如，配置交换机的 Gigabit Ethernet 第一个模块的第一个端口的命令如下：

```
Switch（config）#interface gigabitethernet 1/1
```

若一次指定多个范围段的物理端口，可以使用“range”关键字。每个端口范围段之间用“，”分开，范围段内的连续接口用“－”连接起止编号。

例如，若选择交换机 1、3、11～15 快速以太网端口，则配置命令如下：

```
Switch（config）#interface range fastethernet 0/1，0/3，0/11-15
```

（2）配置端口的 IP 地址和子网掩码

例如，配置路由器端口 serial 0/1 的 IP 地址为 192.168.1.1/24，则配置命令如下：

```
Router（config）#interface serial 0/1
/选择路由器端口 serial 0/1
Router（config-if）#ip address 192.168.1.1 255.255.255.0
/配置路由器端口 serial 0/1 的 IP 地址和子网掩码
```

（3）禁用/启用端口

交换机的所有端口默认是启用的，其状态为 Up，若禁用了某一个端口，则该端口不能收发任何帧，其状态也为 Down；而路由器的端口默认是禁用的，其状态为 Down，启用后，其状态为 Up。在指定的端口配置模式下，配置命令如下：

```
Switch（config-if）#shutdown
/禁用交换机指定端口
Router（config-if）#no shutdown
/启用路由器指定端口
```

（4）查看端口信息

在特权模式下，通常可以使用“show”命令查看网络设备端口的具体信息。

例如，查看路由器端口 serial 0/1 的信息，则配置命令如下：

```
Router（config）#show interface serial 0/1
/查看路由器端口 serial 0/1 的具体信息
```

6.2 虚拟局域网（VLAN）

随着各大机关、学校和企事业单位交换式局域网的大量普及，网络的规模也越来越大，从小型的办公网到大型的园区网，网络管理也变得越来越复杂。首先，在采用共享介质的交换式局域网中，所有节点都处于同一个广播域中，即一个节点向网络中某些节点的广播会被网络中其他节点接收，这样大量的广播报文不仅是对带宽资源和主机处理能力的浪费，而且会因过量的广播产生“广播风暴”，网络信息安全等问题也日益变得突出。其次，当用户由于某些原因在不同网络中移动时，还得重新进行网络连接和网络布线。为了解决此问题可以采用 VLAN 技术。

6.2.1 VLAN 概述

VLAN（Virtual Local Area Network，虚拟局域网）将局域网物理设备从逻辑上划分为多个网段，每个网段对应着一个 VLAN，也就是原来单个广播域虚拟分割成多个广播域，每个广播域就是一个 VLAN，若没有路由的话，一个 VLAN 内部的单播帧、广播帧可以在一个 VLAN 内转发、广播和扩散，而不会直接进入其他的 VLAN 中。也就是说，同一个 VLAN 中的成员都共享广播，形成一个广播域，而不同 VLAN 之间广播信息是相互隔离的，从而有效地控制了流量、减少了设备投资、简化了网络管理、提高了网络之间的安全性。

VLAN 除了能将网络划分为多个广播域，从而有效地控制了“广播风暴”的发生之外，同时，网络管理员又可借助三层交换机或路由器不同 VLAN 之间的路由功能，来管理和控制企业网和园区网中不同管理部门、不同站点之间的信息互访。因此，VLAN 最大的特点是在组成各个逻辑网时无须考虑用户或设备在网络中的物理位置，使网络的拓扑结构变得非常灵活，可以在单个交换机或者跨交换机中实现。

从实现的机制或策略看，VLAN 分为静态 VLAN 和动态 VLAN 两种。静态 VLAN 主要是根据交换机的端口来划分的，动态 VLAN 的划分方法有很多种，常用的主要是根据 MAC 地址划分 VLAN 和根据网络层协议划分 VLAN。

（1）基于端口的 VLAN 划分

这种划分是把一个或多个交换机上的几个端口划分为一个逻辑组（VLAN），这是最简单、最常用和最有效的划分 VLAN 的方法。该方法只需网络管理员对网络设备的交换端口进行重新划分即可，不用考虑该端口所连接的设备，但是美中不足的是以端口为中心

的 VLAN，当 VLAN 用户位置改变时，往往也伴随着用户位置的改变而需要对网线进行迁移。

（2）基于 MAC 地址的 VLAN 划分

这种划分 VLAN 的方法是根据每个主机的 MAC 地址来划分的，即对每个 MAC 地址的主机都配置属于哪个 VLAN。MAC 地址其实就是网卡的标识符，每一块网卡的 MAC 地址都是唯一且固化在网卡上的。MAC 地址由 12 位十六进制数表示，前 6 位为网卡的厂商标识（OUI），后 6 位为网卡标识（NIC）。因此，这种根据 MAC 地址的划分方法其实就是基于用户的 VLAN，最大优点是当用户物理位置发生移动时，VLAN 不需要重新配置；缺点是初始化时，所有的用户都必须进行配置，如果有几百个甚至上千个用户的话，配置就很烦琐。

（3）基于网络层协议的 VLAN 划分

这种划分 VLAN 的方法是根据每个主机的网络层地址或协议类型（如果支持多协议）划分的，目前主要是 IP 地址。 这种方法的优点是用户的物理位置改变了，不需要重新配置所属的 VLAN，而且可以根据协议类型来划分 VLAN，不需要附加的帧标签来识别 VLAN，这样可以减少网络的通信量；缺点是效率低，因为检查每一个数据包的网络层地址是需要消耗处理时间的（相对于前面两种方法）。

6.2.2 基于端口的 VLAN 划分方法

1．创建 VLAN

配置命令如下：

```
Switch（config）#vlan 编号
/创建一个 vlan
Switch（config-vlan）#name 名称
/给 vlan 取一个名称
```

说明：

（1）VLAN 编号是对每个 VLAN 的整数标识，取值范围一般为 1～4094。交换机首次启动，其所有物理接口都属于默认已定义的 VLAN 1。

（2）name 命令是给 VLAN 取一个名称，若没取名称，则交换机会自动命名为 vlan ××××，其中××××是以 0 开头的 4 位 vlan 编号。例如，vlan 0003 就是 vlan 3 的默认名称。

2．向 VLAN 中添加网络接口

配置命令如下：

```
Switch（config）#interface 端口号
/选择单个物理端口
```

```
Switch（config）#interface range 端口号范围段
/选择多个范围段的物理端口
Switch（config-if-range）#switchport access vlan 编号
/把选择的单个或多个范围段的物理端口分配给已创建的 vlan
```

3．删除 VLAN

配置命令如下：

```
Switch（config）#no vlan 编号
/删除指定编号的 vlan
```

说明： VLAN 1 默认存在且不能被删除。

4．查看 VLAN

配置命令如下：

```
Switch#show vlan
/查看创建的 vlan 名称、状态及各 vlan 分配的端口
```

配置实例：如图 6-9 所示，在交换机 Switch 中，划分一个 VLAN 2，命名为 caiwu，并把其接口 FastEthernet 0/11、FastEthernet 0/12 加入这个 VLAN 2 中。

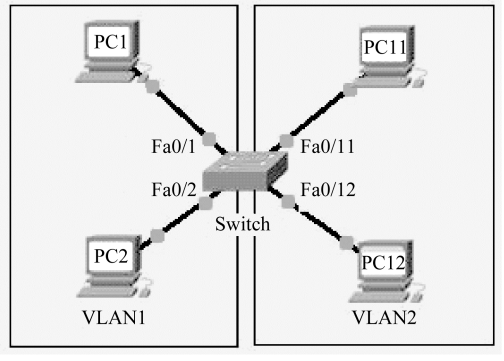


图 6-9　单交换机的 VLAN 划分

提示：

```
Switch（config）#vlan 2
/创建 vlan 2
Switch（config-vlan）#name caiwu
/给 vlan 2 取名为“caiwu”
Switch（config）#interface range fa 0/11，0/12
/选择要分配的端口
Switch（config-if-range）#switchport access vlan 2
```

```
/把选择的端口分配到创建的 vlan 2 中
Switch#show vlan
/查看交换机创建的 vlan 及其分配的端口
```

说明：交换机 Switch 在未配置之前，所有端口都默认在 VLAN1 中，即 PC1、PC2、PC11、PC12 都处于同一个广播域，都可以互访。对交换机 Switch 进行上述配置后，其创建的 VLAN2 中所分配的接口（如 Fa0/11 和 Fa0/12）连接的终端设备（如 PC11 和 PC12）与其默认 VLAN1 中所分配的接口（如 Fa0/1 和 Fa0/2）连接的终端设备（如 PC1 和 PC2）就不能互访了，从而缩小了原来的广播域（VLAN1 的范围变小），起到了隔离网络的目的。

6.2.3 交换机接口的类型

交换机的接口类型一般可分为两大类：二层接口和三层接口。具体如表 6-3 所示。

表 6-3　交换机接口的类型

二层接口	交换接口（Switch Port）	Access Port（接入接口）	交换机默认接口类型，实现二层交换功能，且只能转发来自同一个 VLAN 的帧，但不能配置 IP 地址，没有路由功能
		Trunk Port（干道接口）	实现二层交换功能，可以转发来自多个 VLAN 的帧
	聚合接口（Aggregate Port）	由多个二层低速物理交换接口组成，如同一个高速传输通道的接口	
三层接口	路由接口（Routed Port）	由单个物理接口构成，可配置一个 IP 地址，每个 Routed 接口可用于连接一个子网，Routed 接口的 IP 地址就是该子网的网关。 若一台交换机配置了多个三层接口，则各个三层接口的 IP 地址对应各个不同的网络	
	交换虚拟接口（SVI）	由多个物理 Access 接口组成，但在逻辑上可把它理解为一个三层（网络层）SVI 接口，且每个 SVI 接口可用于连接一个 VLAN，SVI 接口的 IP 地址就是该 VLAN 的网关	

6.2.4 跨交换机 VLAN Trunk 的配置

VLAN Trunk（虚拟局域网中继技术）的作用是让连接在不同交换机上的相同 VLAN 中的主机间互通。例如，交换机 Switch1 的 VLAN1 中的机器要访问交换机 Switch2 的 VLAN1 中的机器，可以分别把两台交换机的级联端口由默认的 Access 端口设置为 Trunk 端口，这样，当交换机把数据包从级联口发出去时，会在数据包中做一个 VLAN 标签（TAG），以使其他交换机能识别该数据包属于哪一个 VLAN，这样，其他交换机收到这样一个数据包后，只会将该数据包转发到标签中指定的 VLAN 中，从而完成了跨交换机相同 VLAN 内部数据的传输。因此，跨交换机相同 VLAN 中的主机相互通信，则交换机与交换机之间的连接接口一般配置为 Trunk 模式（干道模式）。干道就是指两台交换机端口之间的一条点对点连接链路，可以承载多个 VLAN 信息，即 Trunk 端口上可以传送来自不同 VLAN 中发出的数据帧，该端口属于多个 VLAN。

配置实例：如图 6-10 所示，某公司有两层楼，其中一楼的交换机 Switch1 的 FastEthernet 0/24 和二楼的交换机 Switch2 的 FastEthernet 0/24 级联，在 Switch1 和 Switch2 中分别划分了 VLAN2。为了让一楼和二楼相同的 VLAN 的主机可以互访，需分别配置这两个级联口为 Trunk 端口。

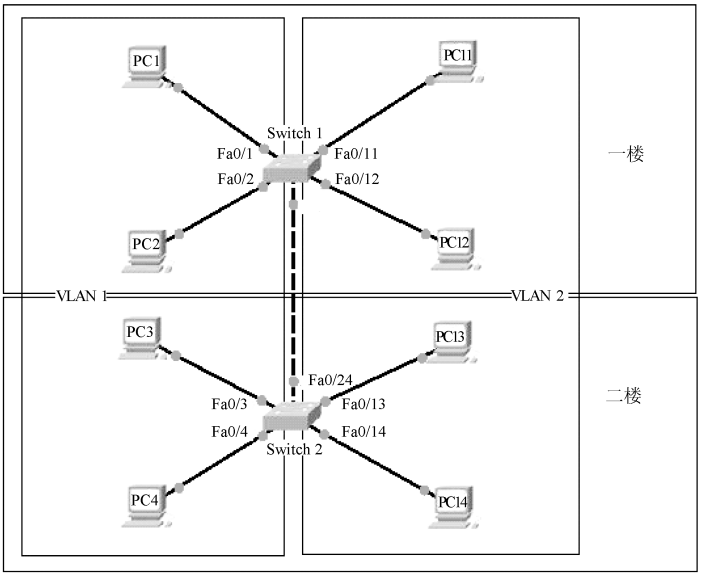


图 6-10　跨交换机的 VLAN 划分

提示：

```
Switch 1（config）#interface 0/24
/选择交换机端口
Switch 1（config-if）#switchport mode trunk
/配置交换机端口模式设置为“Trunk”
```

同理，Switch 2 的 Trunk 端口配置步骤与 Switch 1 一样。

说明：两个交换机的端口 FastEthernet 0/24 未配置前默认工作模式都为“access”，都属于 VLAN1，且只能传输默认 VLAN 1 中的数据，即两个楼层相同 VLAN 1 中的主机是可以互访的，也就是 PC1、PC2、PC3、PC4 同处于一个广播域，是可以互访的。然而，PC11、PC12 和 PC13、PC14 是不可以互访的，因为这几台 PC 连接的端口默认工作模式都为“access”， 且都属于 VLAN 2，而只有配置了这两个级联口工作模式都为“trunk”，才能在此链路上传输 VLAN 2 中的数据，即两个楼层相同 VLAN 2 中的主机才能互访，也就是 PC11、PC12、PC13、PC14 同处于一个广播域，才可以互访了。因此，在默认情况下，交换机的 Trunk 链路是允许所有 VLAN 使用的。

6.2.5 不同 VLAN 间的通信

交换机虚拟接口（Switch Virtual Interface，SVI）代表一个由交换端口构成的 VLAN（其实就是通常所说的 VLAN 接口），也就是一个 SVI 接口对应一个 VLAN。要实现不同 VLAN 之间的通信，就需要借助三层交换机不同的 SVI 接口 IP 地址路由通信功能。那么，首先需要为相应的 VLAN 配置相应的 SVI 接口，其实 SVI 就是指通常所说的 VLAN 接口，只不过它是虚拟的，用于连接整个 VLAN，所以通常也把这种接口称为逻辑三层接口。在全局配置模式下，输入“interface vlan 编号”命令来创建具体 VLAN 的 SVI 接口，指定相应的 IP 地址，就可以通过三层设备的路由功能对数据进行路由转发，实现 VLAN 间的路由。

1．SVI 接口的创建

配置命令如下：

```
Switch（config）#interface vlan 编号
/进入 vlan 的 SVI 接口配置模式
Switch（config-if）#ip address IP 地址 子网掩码
/给 vlan 的 SVI 接口设置 IP 地址和子网掩码
Switch（config-if）#no shutdown
/启用 vlan 的 SVI 接口
```

2．启用三层 IP 路由功能

配置命令如下：

```
Switch（config）#ip routing
/启用三层 IP 路由
```

说明：交换机一般默认未启用三层 IP 路由功能，如果启用此功能，需输入上述命令。

3．查看三层交换机的路由

配置命令如下：

```
Switch#show ip route
/查看三层交换机的路由表信息
```

说明：检查配置的网络是否已经出现在路由表中。

配置实例：如图 6-11 所示，在交换机中划分 VLAN 10 和 VLAN 20，其中 VLAN 10 的 SVI 接口 IP 地址为 192.68.10.1/24，包含 FastEthernet 0/1 和 FastEthernet 0/2 两个接口；VLAN 20 的 SVI 接口 IP 地址为 192.168.20.1/24，包含 FastEthernet 0/11 和 FastEthernet 0/12 两个接口。现在利用交换机的三层功能使 VLAN 10 和 VLAN 20 中的主机能够互访。

提示：

```
Switch（config）#interface vlan 10
/进入 vlan10 的 SVI 接口配置模式
Switch（config-if）#ip address 192.168.10.1 255.255.255.0
```

```
/配置 vlan10 的 SVI 接口 IP 地址和子网掩码
Switch（config）#interface vlan 20
/进入 vlan20 的 SVI 接口配置模式
Switch（config-if）#ip address 192.168.20.1 255.255.255.0
/配置 vlan20 的 SVI 接口 IP 地址和子网掩码
Switch（config）#ip routing
/启用三层路由功能
Switch#show ip route
/查看路由表
```

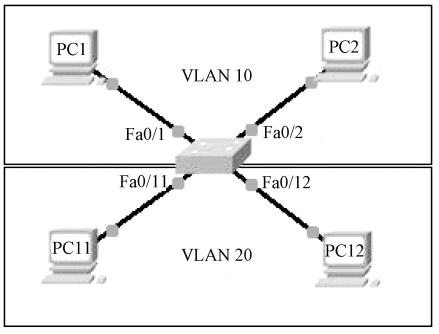


图 6-11　不同 VLAN 间的通信

说明：在本例中，三层交换机 Switch 中已划分了 VLAN 10 和 VLAN 20，即 PC1、PC2 同属于一个广播域 VLAN 10，PC11、PC12 同属于一个广播域 VLAN 20，那么 PC1、PC2 和 PC11、PC12 是不可以互访的。为了实现 VLAN 10 和 VLAN 20 中的主机能够互访，就必须借助三层交换机的路由功能。因此，首先需在三层交换机中分别配置 VLAN 10 和 VLAN 20 三层 SVI 接口的 IP 地址，也就是 VLAN 10 中 PC1、PC2 和 VLAN 20 中 PC11、PC12 的网关。然后用“ip routing”命令开启三层交换机 IP 路由功能，随即可用“show ip route”命令查看路由表。最后可看到三层交换机的路由表中增添了两个路由表项，即 VLAN 10 的 SVI 接口的网络地址段 192.168.10.0/24 和 VLAN 20 的 SVI 接口的网络地址段 192.168.20.0/24，这就说明 VLAN 10 和 VLAN 20 中的主机能够互访了。

6.3　局域网中的冗余链路

在传统的交换式的局域网中，网络设备之间通过单条链路进行连接，当某个节点或某一链路发生故障时，就极有可能导致整个网络无法访问。因此，在实际组建多台交换机组成的网络环境中，通常都会增加一些备份链路（也称为冗余链路），来提高网络的稳定性、可靠性，但备份链路也会使网络生成环路（相同源端和相同目的端的多条路径被称为环路），环路导致数据帧不断地在该多条路径之间传输，将会在网络中产生广播风暴、多帧复制和地址表的不稳定等新问题，直至耗尽所有带宽，导致网络崩溃。

6.3.1 生成树协议原理

生成树协议 STP（Spanning-Tree Protocol）是由 IEEE 802.1d 标准定义的，工作方式如同生成一棵树，即建立无环路连接。其作用是为了解决交换机冗余环路产生“广播风暴”等新问题，而需要在交换机上启动生成树协议来避免此类现象的发生。生成树协议 STP 通过 SPA（生成树算法）使冗余端口置于“阻塞状态”，让网络中的计算机在通信时只有一条链路生效，也就是生成一个无环路的网络，而且当主要链路出现故障时，该协议又会重新计算出网络的最优链路，将处于“阻塞状态”的端口重新打开，从而达到管理冗余链路的目的，保证了网络的正常通信。

生成树协议的工作过程可以归纳为 4 个步骤：选择根网桥；选择根端口；选择指定端口；阻塞非根、非指定端口。

（1）选择根网桥：在全网中选择一个根网桥。

比较网桥的 ID 值，值越小其优先级越高。ID 值是由交换机的优先级和 MAC 地址组成的，如果交换机的优先级相同则比较其 MAC 地址，地址值越小，就被选为根网桥。

（2）选择根端口：在每个非根交换机上选择根端口。

首先，比较根路径成本，根路径成本取决于链路的带宽，带宽越大，路径成本越低，则选该端口为根端口。

其次，如果根路径成本相同，则要比较所在对端交换机 ID 值，值越小，则其优先级越高。

最后，比较端口的 ID 值，该值分为两部分：端口优先级和端口编号，值小的被选为根端口。

（3）选择指定端口：在每条链路上选择一个指定端口，根网桥上所有端口都是指定端口。

首先，比较根路径成本。

其次，比较端口所在网桥的 ID 值。

最后，比较端口的 ID 值。

（4）阻塞非根、非指定端口：在网桥已经确定了根端口和指定端口后，STP 就配置这两种端口转发流量，然后阻塞非根、非指定的端口，形成一个逻辑上无环路的拓扑结构。只有当主链路发生故障时，才会启用备选链路，以保证网络的连通性。

6.3.2 生成树协议的配置

配置命令如下：

```
Switch（config）#spanning-tree
/开启生成树协议
Switch（config）#no spanning-tree
/关闭生成树协议
```

```
Switch（config）#spanning-tree mode { stp |rstp| mstp }
/指定生成树协议的类型
Switch（config）#spanning-tree priority <0-61440>
/配置交换机的优先级
Switch（config-if）#spanning-tree port-priority <0-240>
/配置交换机端口的优先级
Switch（config-if）#spanning-tree cost <cost>
/配置交换机端口的路径成本
Switch#show spanning-tree
/查看生成树配置
Switch#show spanning-tree interface Port-ID
/查看交换机某个具体端口的生成树信息
```

说明：

（1）快速生成树协议 RSTP（Rapid Spanning Tree Protocol）是在 STP 协议基础上做了改进，使得收敛速度快得多（最快 1 秒以内），是按 IEEE 802.1w 标准定义的。

多生成树协议 MSTP（Multiple Spanning Tree Protocol）是在 RSTP 协议上扩展而得到的，它能够通过干道（trunks）建立多个生成树，关联 VLANS 到相关的转发路径。

（2）配置交换机的优先级关系到哪个交换机为整个网络的根交换机，同时也关系到整个网络的拓扑结构。通常情况下，应当把核心交换机的优先级设置得高一些（ID 值小），使之成为根网桥。优先级的设置值为“0”或“4096”的倍数，共 16 个，默认值为 32768。

交换机的优先级要恢复到默认值，可在全局配置模式下输入“no spanning-tree priority”命令实现。

（3）当两个端口都连在一个共享介质上时，交换机会选择一个优先级高（ID 值小）的端口进入转发状态，优先级低（ID 值大）的端口进入丢弃状态。优先级的设置值为“0”或“16”的倍数，共 16 个，默认值为 128。交换机端口的优先级要恢复到默认值，在全局配置模式下输入“no spanning-tree port-priority”命令即可。

（4）交换机会根据哪个端口到根网桥的根路径成本最小来选定根端口，因此，端口路径成本的设置关系到本交换机的哪个端口将成为根端口。端口的链路速率高的成本较小。交换机端口的路径成本的取值范围为 1～200000000。交换机端口的路径成本要恢复到默认值，在全局配置模式下输入“no spanning-tree cost”命令即可。

6.4 端 口 聚 合

随着互联网的不断发展和壮大，运营商们通过提高各自传输网络的综合承载能力来满足更多用户对众多数据业务的传输需求；广大用户也加深了对高网络服务质量的需求，高可用性已经成为当今网络的主要方面。在众多的提高网络可用性的解决方案中，端口聚合技术以增加网络带宽、实现链路负载分担、提高网络可靠性（提供了传输线路内部的冗余

机制）等优点，对数据业务有了很好的支持和完善，在近年来引起了极大的关注并获得迅速发展和广泛应用。

6.4.1 端口聚合概述

端口聚合（也称为链路聚合）是将交换机的多个同类型、低带宽的交换端口捆绑成一条高带宽的复合主干链路，实现了主干链路均衡负载，避免了单条链路出现的拥塞现象。端口聚合就如同超市设置多个收银台以防止收银台过少而出现消费者排队等候时间过长的现象。一般来说，两个普通交换机连接的最大带宽取决于媒介的连接速度（100BAST-TX 双绞线为 200Mbps），而使用 Trunk 技术可以将 4 个 200Mbps 的端口捆绑后成为一个高达 800Mbps 的连接。这一技术的优点是以较低的成本通过捆绑多端口提高带宽，而其增加的开销只是连接用的普通五类网线和多占用的端口，它可以有效地提高子网的上行速度，从而消除网络访问中的瓶颈。另外，如果使用多个端口组成的多条链路，其中的一条链路出现故障，网络传输的数据流可以动态地快速转向其他工作正常的端口组成的链路中而进行传输，对数据起了冗余备份的作用，同时提高了网络的安全性和可靠性。因此，端口聚合技术是可将多物理连接当做一个单一的逻辑连接来处理，它允许两个交换机之间通过多个端口并行连接就如同一条高带宽的链路来传输数据，提供了更高的带宽、更大的吞吐量，增加了冗余、可恢复性。

6.4.2 端口聚合的配置

配置实例：如图 6-12 所示，分别连接交换机 Switch1 的 FastEthernet 0/23 和交换机 Switch2 的 FastEthernet 0/23、交换机 Switch 1 的 FastEthernet 0/24 和交换机 Switch 2 的 FastEthernet 0/24。为了提高两个交换机端口连接的带宽，需要分别把交换机 Switch 1 的 FastEthernet 0/23、FastEthernet 0/24 和 Switch 2 的 FastEthernet 0/23、 FastEthernet 0/24 定义为 AP 端口。

图 6-12　端口聚合的配置

提示：

```
Switch1（config）#interface aggregateport 10
/在交换机上创建一个 AP10 端口
Switch1（config）#interface range fa 0/23，0/24
/选择交换机以太网端口 fa 0/23，0/24
Switch1（config-if-range）#port-group 10
/把选择的以太网端口 fa 0/23，0/24 加入创建的 AP10 端口中
```

说明：Switch 2 的配置步骤与 Switch 1 相同。

6.5 路 由 技 术

伴随着网络规模的不断扩大，路由技术在沟通不同网络连接和实现信息交换方面的应用逐渐被人们所熟知。

路由是指路由器从一个接口上收到数据包，根据数据包的目的地址进行定向并转发到另一个接口的过程。当路由器的某一个接口接收到一个数据包时，会查看包中的目标网络地址以判断该包的目的地址在当前的路由表中是否存在（路由器是否知道到达目标网络的路径）。如果发现包的目标地址与本路由器的某个接口所连接的网络地址相同，那么数据马上转发到相应接口；如果发现包的目标地址不是自己的直连网段，路由器会查看自己的路由表，查找包的目的网络所对应的接口，并从相应的接口转发出去；如果路由表中记录的网络地址与包的目标地址不匹配，则根据路由器配置转发到默认接口，在没有配置默认接口的情况下会给用户返回目标地址不可达的 ICMP 信息并将数据包丢弃。也就是说，路由器查看了数据包的目的协议地址后，确定是否知道如何转发该包，如果路由器不知道如何转发，通常就将之丢弃。如果路由器知道如何转发，就把目的物理地址变成下一跳的物理地址并向之发送。下一跳可能就是最终的目的主机，如果不是，通常为另一个路由器，它将执行同样的步骤。因此，根据 IP地址的网络部分确定数据包的目标网络，并通过 IP 地址的主机部分和设备的 MAC 地址确定到目标节点的连接端口，通过这样一个网络寻址功能使路由器能够在网络中确定一条最佳的路径，然后将数据包从源网络发送至目标网络。

一般来说，根据路由器对路由信息学习、生成并维护路由表的方法，可包括直连路由和非直连路由。

直连路由是由链路层协议发现的，一般指去往路由器的接口地址所在网络的路径，该路径信息不需要网络管理员维护，也不需要路由器通过某种算法进行计算获得，只要该接口处于活动状态，路由器就会自动把通向该网络的路由信息填写到路由表中，因此，路由器能够自动识别路由直连的网络，不需要网络管理员使用命令手工在路由器上配置。

非直连路由是指路由器不能够自动识别的非直连网络，而是通过网络管理员使用命令手工在路由器上配置了路由协议，从其他路由器的路由表中学习到非直连网络的路由。它又可分为静态路由和动态路由两种。

6.5.1 静态路由和默认路由

1．静态路由的概念

静态路由是由网络规划者根据网络拓扑，使用命令手工在路由器上配置的非直连路由信息，这些静态路由信息指导报文发送，静态路由方式也不需要路由器进行计算，不占用路由器的带宽，但是它完全依赖于网络规划者配置。当网络规模较大或网络拓扑经常发生改变时，由于静态路由不能对网络的改变做出及时反映，所以一般用于网络规模不大、拓

扑结构固定的网络中。在所有的路由中，静态路由优先级最高。当动态路由与静态路由发生冲突时，以静态路由为准。因此，静态路由的最大优点就是简单、高效、可靠。

2．静态路由的配置

配置命令如下：

```
Router（config）#ip route 目的网络　子网掩码　出口端口号{下一跳一级端口的 IP 地址 }
/手工定义传输路径，即静态路由
```

说明：

（1）删除已配置的静态路由信息，只需在原有配置命令前加“no”。

（2）配置完成后，可以使用 show ip route 命令查看路由表。

3．默认路由的配置

配置命令如下：

```
Router（config）#ip route 0.0.0.0 0.0.0.0 出口端口号{下一跳一级端口的 IP 地址 }
```

说明：

（1）默认路由又称为默认静态路由，是静态路由的特例，它表示把所有本机不能处理的数据报发往指定的设备。

（2）0.0.0.0　0.0.0.0 表示所有任意目的地址，ip-address 是到达目的地址本机出口的下一跳接口地址。

（3）默认路由的优先级是最低的，设备首先会匹配其他的路由，只有当所有路由条目中没有相匹配的网络地址时，才按照默认路由所指向的网关发送。

（4）在自治系统接入互联网的边界路由器上通常要配置一条默认路由，使所有发往互联网的数据都从这个路由器的网络接口上发送出去。

配置实例：如图 6-13 所示，分别配置 R1 和 R2 的静态路由，使 PC1 与 PC2 能够互通。

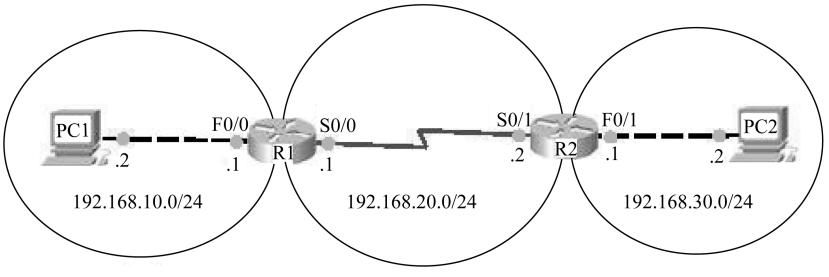


图 6-13　静态路由实例

提示：

```
R1（config）#ip route 192.168.30.0 255.255.255.0 192.168.20.2
或 R1（config）#ip route 192.168.30.0 255.255.255.0 serial 0/0
```

```
R2（config）#ip route 192.168.10.0 255.255.255.0 192.168.20.1
或 R2（config）#ip route 192.168.30.0 255.255.255.0 serial 0/1
```

说明：本例中，R1 通过两个端口 F0/0 和 S0/0 直连的网络为 192.168.10.0/24 和 192.168.20.0/24，随即自动在 R1 路由表中生成两个路由表项。因此，这两个直连网络不需要手工配置指定；而非直连网络 192.168.30.0/24，需在 R1 中手工配置此目标网络的静态路由信息，然后用“show ip route”命令查看路由表，可看到 R1 路由表中又增添了一个路由表项，即非直连网络 192.168.30.0/24；同理，R2 通过两个端口 F0/1 和 S0/1 直连的网络为 192.168.30.0/24 和 192.168.20.0/24，随即自动在 R2 路由表中生成两个路由表项。因此，这两个直连网络不需要手工配置指定；而非直连网络 192.168.10.0/24，需在 R1 中手工配置此目标网络的静态路由信息，然后用“show ip route”命令查看路由表，可看到 R2 路由表中又增添了一个路由表项，即非直连网络 192.168.10.0/24。最后，设置 PC1、PC2 的网关，那么 PC1 和 PC2 就可以互访了。

注意：设置 PC1 的网关为 R1 端口 F0/0 的 IP 地址：192.168.10.1；设置 PC2 的网关为 R2 端口 F0/1 的 IP 地址：192.168.30.1。

6.5.2 动态路由协议

动态路由是网络中的路由器之间根据实时网络拓扑变化，相互通信传递路由信息，利用收到的路由信息通过路由选择协议计算，更新路由表的过程。因此，动态路由减少了许多管理任务。根据是否在一个自治域（指一个具有统一管理机构、统一路由策略的网络）内部使用，动态路由协议分为内部网关协议（IGP）和外部网关协议（EGP）。自治域内部采用的路由选择协议称为内部网关协议，常用的有路由信息协议 RIP（Routing Information Protocol）、开放式最短路径优先OSPF（Open Shortest Path First）协议；外部网关协议主要用于多个自治域之间的路由选择，常用的是 BGP 和 BGP-4。其中，IGP 又分为距离矢量路由协议和链路状态路由协议（如 OSPF）。

距离矢量路由协议计算网络中所有链路的矢量和距离并以此为依据确认最佳路径。使用距离矢量路由协议的路由器会定期向其相邻的路由器发送全部或部分路由表，如 RIP。

链路状态路由协议使用为每个路由器创建的拓扑数据库来创建路由表，每个路由器通过此数据库建立一个整个网络的拓扑图。在拓扑图的基础上通过相应的路由算法计算出通往各目标网络的最佳路径，并最终形成路由表。

6.5.3 RIP 协议

1．RIP 协议的概念

路由信息协议是应用较早、使用较普遍的内部网关协议，是典型的距离向量路由选择协议。当网络中每台路由器启动后，会把自己直连的网络写到路由表中，同时每隔 30s 会将自己生成的路由表广播或者组播给相邻路由器，并监听相邻路由器发来的路由表，经过层

层相互交换学习，每个路由器最终会学习到所有网络的信息，并根据距离矢量算法得到一条到达每一个目标网络的最佳路径。RIP 采用距离矢量算法，即路由器根据它跳过的路由器的数目最少（“距离最短”）来作为度量标准确定到达目的地的最佳路由。RIP 协议允许一条路径最大跳数是 15，因此，距离为 16 时即不可到达。由此可见，RIP 协议的缺点：一方面，周期性地发布路由表，带来不必要的流量；另一方面，路由器不清楚整个网络的拓扑结构，只知道和自己直连的网络情况，对网络变化收敛速度慢，且存在路由环路的问题，不适用于大型的复杂网络。

2．RIP 协议配置

配置实例：如图 6-14 所示，分别配置 R1 和 R2 的 RIP 路由协议，使 PC1 与 PC2 能够互通。

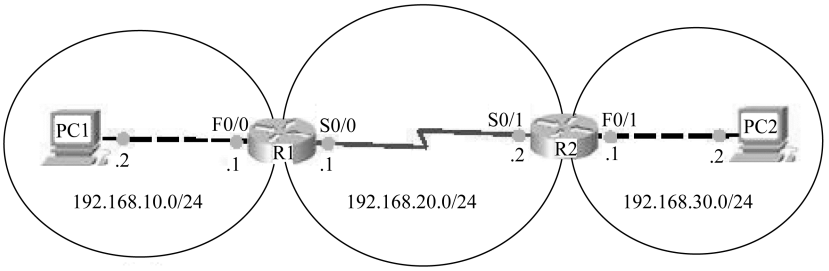


图 6-14　RIP 协议配置实例

提示：

```
R1（config）#router rip
/启用 R1 的 RIP 协议，并进入 RIP 路由配置模式
R1（config-router）#network 192.168.10.0
/指定 R1 中直接参与 RIP 路由协议的网络地址
R1（config-router）#network 192.168.20.0
/指定 R1 中直接参与 RIP 路由协议的网络地址
R2（config）#router rip
/启用 R2 的 RIP 协议，并进入 RIP 路由配置模式
R2（config-router）#network 192.168.20.0
/指定 R2 中直接参与 RIP 路由协议的网络地址
R2（config-router）#network 192.168.30.0
/指定 R2 中直接参与 RIP 路由协议的网络地址
```

说明：R1 启用了 RIP 协议后就会把两个端口直连的目标网络地址 192.168.10.0/24 和 192.168.20.0/24 存到自己的路由表中，且跳数都为 0（管理距离都为 0）；R2 启用了 RIP 协议后同样也会把两个端口直连的目标网络地址 192.168.20.0/24 和 192.168.30.0/24 存到自己的路由表中，且跳数都为 0（管理距离都为 0）。按照 RIP 协议，隔 30sR1 和 R2 就开始相互学习路由表，没有的目标网络地址就会自动学习到各自的路由表中。因此，在 R1 的路由表中也就很快增加了 192.168.30.0/24 目标网络地址，跳数为 1（管理距离为 1）；同样，R2 的

路由表中也就很快增加了 192.168.10.0/24 目标网络地址，跳数为 1（管理距离为 1）。由此可见，运行 RIP 协议的路由器就是依靠和邻居之间周期性地交换路由表，从而一步步学习到远端的路由。

6.5.4 OSPF 协议

1．OSPF 协议的概念

OSPF 是一种链路状态的路由协议，需要每个路由器向其同一管理域的所有其他路由器发送链路状态广播信息。在 OSPF 的链路状态广播中包括所有接口信息、所有的量度和其他一些变量。利用 OSPF 的路由器首先必须收集有关的链路状态信息，并根据一定的算法计算出到每个节点的最短路径。

与 RIP 不同，OSPF 将一个自治域再划分为区，相应地，即有两种类型的路由选择方式：当源和目的地在同一区时，采用区内路由选择；当源和目的地在不同区时，则采用区间路由选择。这就大大减少了网络开销，并增加了网络的稳定性。当一个区内的路由器出了故障时并不影响自治域内其他区路由器的正常工作，这也给网络的管理、维护带来了方便。由此可见，OSPF 协议是用链路状态来评估路由，可用于规模较大的网络。

2．OSPF 协议配置

配置实例：如图 6-15 所示，分别配置 R1 和 R2 的 OSPF 路由协议，使 PC1 与 PC2 能够互通。

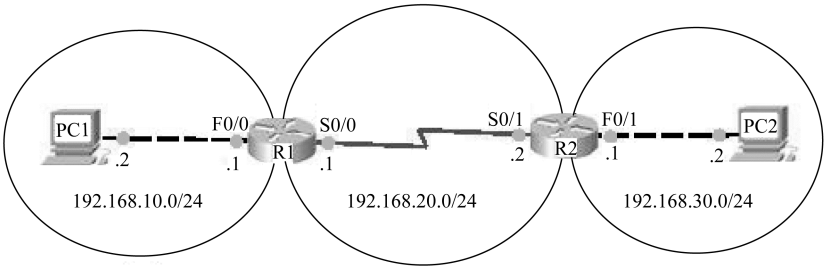


图 6-15　OSPF 协议配置实例

提示：

```
R1（config）#router ospf 1
/启用 OSPF 协议，并进入 OSPF 路由配置模式
R1（config-router）#network 192.168.10.0 0.0.0.255 area 0
/在区域内指定直接参与该路由器 OSPF 路由的网络地址及其通配符掩码
R1（config-router）#network 192.168.20.0 0.0.0.255 area 0
R2（config）#router ospf 1
/启用 OSPF 协议，并进入 OSPF 路由配置模式
R2（config-router）#network 192.168.20.0 0.0.0.255 area 0
/在区域内指定直接参与该路由器 OSPF 路由的网络地址及其通配符掩码
```

```
R2（config-router）#network 192.168.30.0 0.0.0.255 area 0
```

说明：本例中，R1 通过两个端口 F0/0 和 S0/0 直连的网络为 192.168.10.0/24 和 192.168.20.0/24，随即自动在 R1 路由表中生成两个路由表项；R2 通过两个端口 F0/1 和 S0/1 直连的网络为 192.168.30.0/24 和 192.168.20.0/24，随即自动在 R2 路由表中生成两个路由表项。首先在骨干网区域（area 0）内，R1、R2 通过启用动态 OSPF 协议，然后用“show ip route”命令查看路由表，随即看到 R1 路由表中又增加了 R2 路由表中的 192.168.30.0/24 路由表项；R2 路由表中又增加了 R1 路由表中的 192.168.10.0/24 路由表项。最后，设置 PC1、PC2 的网关，那么 PC1 和 PC2 就可以互访了。

注意：设置 PC1 的网关为 R1 端口 F0/0 的 IP 地址：192.168.10.1；设置 PC2 的网关为 R2 端口 F0/1 的 IP 地址：192.168.30.1。

6.6　网络信息安全

随着计算机技术的飞速发展，信息网络已经成为社会发展的重要保证。信息网络涉及国家的政治、军事、文教等诸多领域，存储、传输和处理的许多信息是政府宏观调控决策、商业经济信息、银行资金转账、股票证券、能源资源数据、科研数据等重要的信息。其中有很多是敏感信息，甚至是国家机密，所以难免会吸引来自世界各地的各种人为攻击（如设备入侵、信息泄露、信息窃取、病毒传播等），那么网络信息安全面临更大挑战，而通过交换机端口安全、配置访问控制列表 ACL、在防火墙实现包过滤及入侵检测甚至防毒功能等一些常用的网络设备安全防护技术就变得尤为重要。

6.6.1　交换机端口安全

1．端口安全概述

端口安全是一种基于 MAC 地址的安全机制。这种机制通过检测数据帧中的源 MAC 地址来控制非授权设备对网络的访问，通过检测数据帧中的目的 MAC 地址来控制对非授权设备的访问。在网络设备启动了端口安全功能之后，当发现非法报文时，系统将触发相应特性，通过预先配置的行为方式自动进行违规处理，以减少用户的维护工作量，提高了系统的安全性和可管理性。端口安全的主要功能是通过定义各种端口安全模式，让设备学习到合法的源 MAC 地址，以达到相应的网络管理效果。它主要有以下几个功能。

（1）允许特定 MAC 地址的网络设备接入网络，从而防止用户将非法或未授权的设备接入网络。

（2）限制端口接入的设备数量，防止用户将过多的设备接入网络中。

2．端口安全的配置

交换机作为网络的接入设备，通过在交换机某个端口上限制接入设备的 MAC 地址或 IP

地址，来控制对该端口的接入访问功能，从而进行对接入网络用户的区分。为了增强网络的安全性，还可以将 MAC 地址和具体的端口 IP 地址一起绑定起来作为安全地址，来限制接入用户的混乱连接。交换机端口配置了安全功能后，即配置了安全地址，如果该端口收到的源地址不是安全地址的数据，即发现主机的 MAC 地址与交换机上端口指定的 MAC 地址不同时，交换机相应的端口不转发该数据包，并产生一个安全违例，让用户可以选择多种方式来处理该安全违例，如丢弃接收到的数据包，发送安全违例通知或关闭相应端口。

交换机的端口安全还表现在可以限制具体端口通过 MAC 地址的数量，以防止利用交换机端口的广播功能，私自连接设备扩展网络，造成网络的流量过大。如果交换机的端口上接收到的安全地址数量超过了该端口允许的最大数量，则该端口不转发该数据包，并产生一个安全违例，让用户可以选择多种方式来处理该安全违例，如丢弃接收到的数据包，发送安全违例通知或关闭相应端口。

交换机端口安全配置思路大概分为三步：一是配置端口的安全策略；二是指定授权访问的设备的 MAC 地址；三是配置端口安全违例后的处理。

（1）MAC 地址与端口的绑定

配置命令如下：

```
Switch（config）#interface 端口号
/指定交换机某一端口
Switch（config-if）#switchport mode access
/指定此端口为 access 模式，默认为此模式
Switch（config-if）#switchport port-security mac-address MAC 地址
/为此端口配置 MAC 地址
```

（2）通过 MAC 地址来限制端口流量

配置命令如下：

```
Switch（config）#interface 端口号
/指定交换机某一端口
Switch（config-if）#switchport trunk encapsulation dot1q
/指定此端口 trunk 模式封装协议为 dot1q
Switch（config-if）#switchport mode trunk
/配置端口模式为 trunk
Switch（config-if）#switchport port-security maximum 数值
/允许此 trunk 端口通过的最大 MAC 地址数
```

（3）端口的三种违例处理方式

配置命令如下：

```
Switch（config-if）#switchport port-security violation{protect|restrict
|shutdown}
/指定端口违例处理的三种方式
```

说明：交换机端口的三种违例处理方式，即基于上述情况（1）和（2）违规发生后的动作：

① protect——保护方式，直接丢弃违例主机的数据包，不发出警告。

② restrict——限制方式，不转发主机的数据包，向网络管理主机发出通知。

③ shutdown——禁用端口方式，当违例产生时，马上关闭端口并发出一个通知。

6.6.2 访问控制列表（ACL）

信息点间通信和内外网络的通信都是企业网络中必不可少的业务需求，但是为了保证内网的安全性，通常需要通过在网络设备上实施一些安全策略来保障非授权用户只能访问特定的网络资源，从而达到对访问进行控制的目的。访问控制是网络安全防范和保护的主要策略，也是保证网络安全最重要的核心策略之一。访问控制涉及的技术也比较广泛，包括入网访问控制、网络权限控制、目录级控制及属性控制等。它的主要功能就是：一方面保护网络资源不被非法使用和访问；另一方面限制特定用户访问网络的权限。

1．ACL 概述

访问控制列表（Access Control List，ACL）是由 permit 或 deny 语句组成系统有顺序的规则列表，这些规则根据数据包的源地址、目标地址、端口号等来描述，ACL 通过这些规则对数据包进行分类，并将规则应用到路由器的某个接口上，这样路由器就可以根据这些规则来判断哪些数据包可以接收，哪些数据包需要拒绝，从而实现网络的安全性。

当然路由器上默认是没有 ACL 的，也就是说在默认情况下允许任何数据包通过路由器。就如同一个单位没有保安，那么任何人出入单位都不会受到限制，这样就会给单位的财产带来不安全的因素。因此，可以在单位门口设置一个保安，那么这个保安就会看是否是本单位的人。若是本单位的人进入，直接通过；若不是就要盘问一番，确定是否拒绝进入。同理，也可以在路由器的某个接口上定义一个列表，检查通过该接口上的每一个数据包，符合某个条件的通过，或者是符合某个条件的不允许通过，从而实现对数据包过滤的作用。因此，作为外网进入企业内网的第一道关卡，路由器上的访问控制列表不但可以对网络流量、流向起到控制的作用，而且在很大程度上成为保护内网安全的有效手段，也是保证整个网络安全最重要的核心安全策略之一。

ACL 安全控制技术根据其控制网络范围的精细程度不同，主要分为标准 IP ACL（Standard IP ACL）和扩展 IP ACL（Extended IP ACL）两种类型。ACL 安全控制主要执行的两个动作为允许（Permit）和拒绝（Deny），应用在路由器上主要是在端口的输入（In）和输出（Out）两个方向上的应用。

2．定义 IP ACL

（1）标准 IP ACL

如果需要阻止来自某一个网络的所有数据流，或者允许来自某一特定网络的所有数据流，可以在路由器中配置标准 IP ACL 来实现这一目标。配置标准 IP ACL 的路由器，会检查收到的数据包的源地址是否匹配标准 IP ACL 语句，从而执行允许或拒绝此网络地址的所有数据流通过路由器的端口。

配置命令如下：

```
Router（config）#access-list 列表号 {permit|deny}[定义过滤源主机范围]
```

说明：

① 标准 IP ACL 列表号取值范围为 1～99。

② 关键字 permit 表示允许从该端口通过流量，deny 表示拒绝从该端口通过流量。

③ 过滤源主机范围可以是源主机的 IP 地址（host ip 地址），也可以是源网络地址（源网络地址 通配符掩码）。

④ 若过滤源主机范围为“0.0.0.0 255.255.255.255”，可以用关键字“any”来代替。

⑤ 若过滤源主机范围为“IP 地址 0.0.0.0”， 可以用关键字“host ip 地址”来代替。

（2）扩展 IP ACL

配置扩展 IP ACL 的路由器既检查数据包的源地址信息，也检查数据包的目的地址信息，还检查数据包中特定的协议类型、端口号、时间段等信息。因此，扩展 IP ACL 比标准 IP ACL 有更多的匹配项，更具有灵活性和可扩充性，在安全控制功能上，也更加精细和具体。

配置命令如下：

```
Router（config）#access-list 列表号 {permit|deny} [协议][定义过滤源主机范围][定义过滤源端口][定义过滤目的主机范围][定义过滤目的端口]
```

说明：

① 扩展 IP ACL 列表号取值范围为 100～199。

② 关键字 permit 表示允许从该端口通过流量，deny 表示拒绝从该端口通过流量。

③ 协议定义了需要被过滤的协议，如 IP、TCP。

④ 过滤源主机范围可以是源主机的 IP 地址（host ip 地址），也可以是源网络地址（源网络地址 通配符掩码）。

⑤ 在 ACL 中规定通配符掩码用反向掩码来表示子网掩码。

⑥ 若过滤源主机范围为“0.0.0.0 255.255.255.255”，可以用关键字“any”来代替。

⑦ 若过滤源主机范围为“IP 地址 0.0.0.0”， 可以用关键字“host ip 地址”来代替。

⑧ 定义过滤目的主机范围与过滤源主机范围的结构相同。

⑨ 定义过滤端口可以使用数字或可识别的助记符表示各种条件。

3．IP ACL 应用到端口上

为路由器指定一个端口，并将配置好的标准 IP ACL 或者扩展 IP ACL 应用到该端口上，使其对输入或输出端口的数据流进行安全接入控制。

配置命令如下：

```
Router（config）#interface 端口号
Router（config-if）#ip access-group 列表号 {in|out}
```

说明：

① interface 命令用于指定 IP ACL 应用的端口。

② “端口号”是端口名称，一般表示方法：“端口类型 插槽号/接口号”。

③ in|out 用来指定该 ACL 是被应用到流入端口（in），还是流出端口（out）。

网络环境：如图 6-16 所示，路由器R1 连接了两个网段，分别为 172.16.1.0/24 和 172.16.2.0/24。在 172.16.2.0/24 网段中有一台服务器Server 提供 WWW 服务，IP 地址为 172.16.2.12。

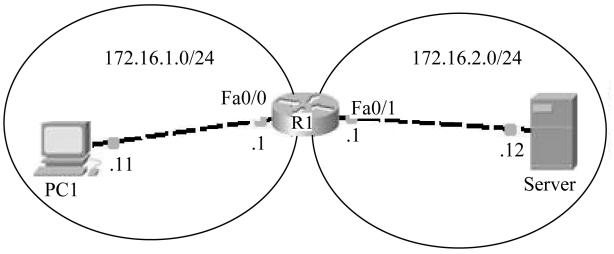


图 6-16　访问控制列表实例

配置实例 1：如图 6-16 所示，禁止 172.16.2.0/24 网段中的计算机除 Server 这台服务器以外访问 172.16.1.0/24 的计算机。172.16.2.12 可以正常访问 172.16.1.0/24。

提示：

```
R1（config）# access-list 1 permit host 172.16.2.12
/配置 ACL1，允许 172.16.2.12 的数据包通过
R1（config）#access-list 1 deny any
/配置 ACL1，拒绝其他一切 IP 地址进行通信
R1（config）#int fa 0/1
/进入 fa 0/1 端口
R1（config-if）#ip access-group 1 in
/将 ACL1 应用在此端口上
```

说明：经过设置后 R1 端口就只允许来自 172.16.2.12 这个 IP 地址的数据包传输了，而来自其他 IP 地址的数据包都无法通过 R1 传输。

配置实例 2：如图 6-16 所示，禁止 Server 这台服务器对 172.16.1.0/24 网段的访问，而 172.16.2.0/24 中的其他计算机可以正常访问。

提示：

```
R1（config）#access-list 1 deny host 172.16.2.12
/设置 ACL1，禁止 172.16.2.12 的数据包通过
R1（config）#access-list 1 permit any
/设置 ACL1，允许其他地址的计算机进行通信
R1（config）#int fa 0/1
/进入 fa 0/1 端口
R1（config-if）#ip access-group 1 in
```

```
    /将 ACL1 应用在 fa 0/1 端口上，同理可以进入 fa 0/0 端口后使用 ip access-group 1 out
命令来完成配置
```

说明：配置完毕后除了 172.16.2.12 以外，其他 IP 地址都可以通过路由器正常通信。

配置实例 3：如图 6-16 所示，禁止 172.16.1.0 的计算机访问 172.16.2.0 的计算机，包括 Server 这台服务器，不过唯独可以访问 Server 上的 WWW 服务，而其他服务不能访问。

提示：

```
    R1（config）#access-list 101 permit tcp any 172.16.2.12 0.0.0.0 eq www
    /设置 ACL101，允许源地址为任意 IP，目的地址为服务器 Server 的 80 端口，即 WWW 服务。由于
路由器默认添加 deny any 命令，所以 ACL 只写此一句即可
    R1（config）#int fa 0/1
    /进入 fa 0/1 端口
    R1（config-if）#ip access-group 101 out
    /将 ACL101 应用到 fa 0/1 出口上
```

说明：设置完毕后 172.16.1.0 的计算机就无法访问 172.16.2.0 的计算机了，就算是服务器 172.16.2.12 开启了 FTP 服务也无法访问，唯独可以访问的就是 Server 的 WWW 服务，而 172.16.2.0 网段中的计算机可以访问 172.16.1.0 网段中的计算机。

6.7 网络地址转换（NAT）

随着接入 Internet 的计算机数量的不断猛增，IP 地址资源也就愈加显得捉襟见肘。事实上，除了中国教育和科研计算机网（CERNET）外，一般用户几乎申请不到整段的 C 类 IP 地址。在其他 ISP 那里，即使是拥有几百台计算机的大型局域网用户，当他们申请 IP 地址时，所分配的地址也不过只有几个或十几个 IP。显然，这样少的 IP 地址根本无法满足网络用户的需求，于是也就产生了 NAT 技术。

6.7.1 私有地址

Internet 上有成千上万台主机，为了区分这些主机，人们给每台主机分配了专门的地址，称为 IP 地址。通过 IP 地址可以访问到网络上的每一台主机。IP 地址分为公有地址和私有地址两种，但只有公有地址才能在 Internet 上进行通信，私有地址不能直接在公网上使用，只能在内部私有网络中使用。因此，私有（保留）地址是当时国际组织分配 IP 地址时保留（不需要经过申请注册）下来的一部分地址，用于给一个组织网络内部的计算机使用。根据 IP 网络协议，在前三类 IP 地址中都有一个网络号是保留的 IP 地址，不需要申请注册，只能在内部私有网络中使用。具体分布如下：

① A 类：10.0.0.0/8。

② B 类：172.16.0.0/16。

③ C 类：192.168.0.0/24。

6.7.2 NAT 的概念

网络地址转换，即 NAT（Network Address Translation）功能，就是指在一个组织网络内部，各计算机间通过私有 IP 地址进行通信，而当组织内部的计算机要与外部 Internet 网络进行通信时，具有 NAT 功能的设备（这里路由器）负责将其私有 IP 地址转换为真的 IP 地址，即该组织申请的合法 IP 地址才能进行通信。

简单地说，NAT 就是一种将私有（保留）地址转换为合法 IP 地址的接入广域网技术。这种技术不仅解决了 IP 地址不足的问题，而且能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机，提高了网络的安全性。

6.7.3 NAT 原理

当内部网络有多台主机访问互联网上的多个目的主机时，路由器必须记住内部网络的哪一台主机访问互联网上的哪一台主机，以防止在地址转换时将不同的连接混淆，所以路由器会为 NAT 的众多连接建立一个表，即 NAT 表。

NAT 在做地址转换时，依靠在 NAT 表中记录内部私有地址和外部公有地址的映射关系来保存地址转换的依据。当执行 NAT 操作时，路由器在做某一数据连接操作时只需要查询该表，就可以得知应该如何转换地址，而不会发生数据连接的混淆。

NAT 表中每一个连接条目，都有一个计时器。当有数据在这两台主机之间传递时，数据包不断刷新 NAT 表中的相应条目，则该条目将处于不断被激活的状态，该条目不会被 NAT 表清除。但是，如果两台主机长时间没有数据交互，则在计时器倒数到零时，NAT 表将把这一条目清除。

在运行 NAT 的路由器中，当数据包被传送时，NAT 可以转换数据包的 IP 地址和 TCP/UDP 数据包的端口号。设置 NAT 功能的路由器至少要有一个 Inside（内部）端口和一个 Outside（外部）端口。内部端口连接内网的用户，外部端口一般连接到 Internet。当 IP 数据包离开内部网络时，NAT 负责将内网 IP 源地址（通常是专用地址）转换为合法的公共 IP 地址。当 IP 数据包进入内网时，NAT 将合法的公共 IP 目的地址转换为内网的 IP 源地址，如图 6-17 所示。

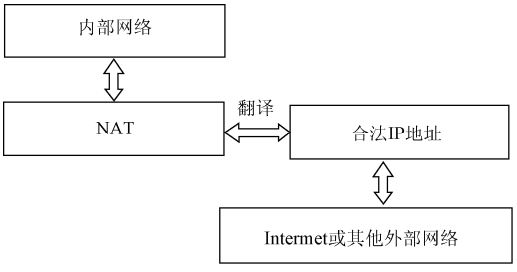


图 6-17　网络地址转换原理

6.7.4 NAT 的配置

NAT 按实现方式有三种，即静态 NAT、动态 NAT 和端口复用动态 NAT。

1．静态 NAT

静态网络地址转换（Static NAT）是指将内部网络的私有 IP 地址转换为公有 IP 地址，IP 地址对是一对一的，是一成不变的，某个私有 IP 地址只转换为某个公有 IP 地址。借助于静态转换，可以实现外部网络对内部网络中某些特定设备（如服务器）的访问。

配置实例 1：某公司想让外部用户访问一台内部网络的 Web 服务器，管理员可以在路由器 Router 中使用静态 NAT，将一个外网全球地址（2.2.2.3）映射到一个内部地址（10.0.0.10），假设该路由器 Router 的 Fa0/0 端口连接内网，Fa 0/1 端口连接外网。

提示：

（1）定义内部接口，连接内部网络：

```
Router（config）#int fa 0/0
Router（config-if）#ip address 10.0.0.10 255.0.0.0
Router（config-if）#ip nat inside
/定义该端口连接内网
```

（2）定义外部接口，连接外部网络：

```
Router（config-if）#int fa 0/1
Router（config-if）#ip address 2.2.2.3 255.0.0.0
Router（config-if）#ip nat outside
```

（3）在内部本地地址与外部全局地址之间建立静态网络地址转换：

```
Router（config）#ip nat inside source static 10.0.0.10 2.2.2.3
```

2．动态 NAT

动态网络地址转换（Dynamic NAT）是指将内部网络的私有 IP 地址转换为公有 IP 地址，IP 地址是不确定的，是随机的，所有被授权访问 Internet 的私有 IP 地址可随机转换为任何指定的合法 IP 地址。也就是说，只要指定哪些内部地址可以进行转换，以及用哪些合法地址作为外部地址时，就可以进行动态转换。动态转换可以使用多个合法外部地址集。当 ISP 提供的合法 IP 地址略少于网络内部的计算机数量时，可以采用动态转换的方式。

配置实例 2：某公司想让外部用户访问内部网络的主机，管理员可以在路由器 Router 中使用动态 NAT，将一个外网全球地址（2.2.2.1～2.2.2.3）映射到内部网络地址（10.0.0.0）上，假设路由器 Router 的 Fa 0/0 端口连接内网，Fa 0/1 端口连接外网。

提示：

（1）定义内部端口，连接内部网络：

```
Router（config）#int fa 0/0
Router（config-if）#ip address 10.0.0.0 255.0.0.0
Router（config-if）#ip nat inside
```

（2）定义外部端口，连接外部网络：

```
Router（config-if）#int fa 0/1
Router（config-if）#ip address 2.2.2.1 255.0.0.0
Router（config-if）#ip nat outside
```

（3）定义合法 IP 地址池：

```
Router（config）#ip nat pool mynatpool 2.2.2.1 2.2.2.3 netmask 255.255.255.0
```

（4）定义一个标准 ACL，允许哪些内部地址可以进行动态地址转换：

```
Router（config）#access-list 1 permit 10.0.0.0 0.0.0.255
```

（5）实现网络地址转换：将由 access-list 指定的内部本地地址与指定的外部合法地址进行地址转换。

```
Router（config）#ip nat inside source list 1 pool myanatpool
```

3．端口复用动态 NAT

端口多路复用是指改变外出数据包的源端口并进行端口转换，即端口地址转换（Port Address Translation，PAT），采用端口多路复用方式。内部网络的所有主机均可共享一个合法外部 IP 地址实现对 Internet 的访问，从而可以最大限度地节约 IP 地址资源。同时，又可隐藏网络内部的所有主机，有效避免来自 Internet 的攻击。因此，目前网络中应用最多的就是端口多路复用方式。

配置实例 3：某公司想让外部用户访问内部网络的主机，管理员可以在路由器 Router 中使用端口复用动态 NAT，将一个外网全球地址（2.2.2.1～2.2.2.3）映射到内部网络地址（10.0.0.0）上，假设路由器 Router 的 Fa 0/0 端口连接内网，Fa 0/1 端口连接外网。

提示：

（1）定义内部端口，连接内部网络：

```
Router（config）#int fa 0/0
Router（config-if）#ip address 10.0.0.0 255.0.0.0
Router（config-if）#ip nat inside
```

（2）定义外部端口，连接外部网络：

```
Router（config-if）#int fa 0/1
Router（config-if）#ip address 2.2.2.1 255.0.0.0
Router（config-if）#ip nat outside
```

（3）定义合法 IP 地址池：

```
Router（config）#ip nat pool mynatpool 2.2.2.1 2.2.2.100 netmask 255.255.255.0
```

（4）定义一个标准 ACL，允许哪些内部地址可以进行动态地址转换：

```
Router（config）#access-list 1 permit 10.0.0.0 0.0.0.255
```

（5）实现网络地址转换：将由 access-list 指定的内部本地地址与指定的外部合法地址进行地址转换：

```
Router（config）#ip nat inside source list 1 pool myanatpool overload
```

6.8 网络规划与设计

网络规划与设计就是在组网之前对整个网络需求进行可行性分析，根据分析设计网络拓扑结构，选择合适的组网技术，选用和配置网络设备，以实现 Intranet、Internet 的连接和各种网络应用功能。

6.8.1 网络拓扑结构

拓扑学（Topology）是一种研究与大小、距离无关的几何图形特性的方法。网络拓扑是由网络节点设备和通信介质相互连接的网络结构图，它反映了网络中各实体间的结构关系。因此，网络拓扑结构设计的好坏对整个网络的性能和经济性都有重大影响。目前主要有总线型结构、星型结构、环型结构、分布式结构、树型结构、网状结构和蜂窝状结构。

6.8.2 层次化网络结构设计

网络拓扑结构设计常采用层次化的方法。层次化网络设计在互联网组件的通信中引入了三个关键层的概念，这三个层次分别是：核心层（Core Layer）、汇聚层（Distribution Layer）和接入层（Access Layer），如图 6-18 所示。

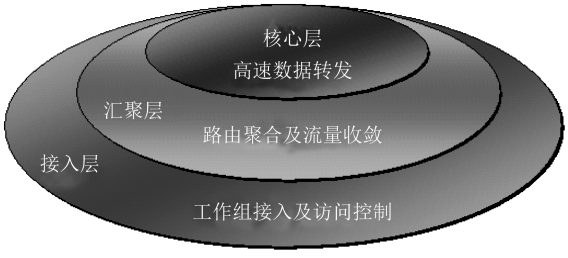


图 6-18　层次化网络结构设计

1．核心层

核心层的功能主要是实现骨干网络之间的优化传输，骨干层设计任务的重点通常是冗余能力、可靠性和高速的传输，而网络的控制功能最好尽量少在骨干层上实施。核心层一直被认为是所有流量的最终承受者和汇聚者，所以对核心层的设计以及网络设备的要求十分严格。因此，核心层不但需要考虑冗余设计，而且其设备将占投资的主要部分。

2．汇聚层

汇聚层是楼群或小区的信息汇聚点，是连接接入层节点和核心层的中心，为接入层提供数据的汇聚、传输、管理、分发处理和基于安全管理综合策略的连接，如地址合并、协议过滤、路由服务、认证管理等，通过网段划分（如 VLAN）与网络隔离可以防止某些网段的问题蔓延和影响到核心层。汇聚层同时也可以提供接入层虚拟网之间的互联，控制和限制接入层对核心层的访问，保证核心层的安全和稳定。

汇聚层设备一般需要较高的性能和较丰富的功能，一般采用可管理的三层交换机或堆叠式交换机。汇聚层设备之间以及汇聚层设备与核心层设备之间多采用光纤互联，以提高系统的传输性能和吞吐量。

3．接入层

接入层通常指网络中直接面向用户连接或访问的部分，其主要功能是完成用户流量的接入和隔离。因此，接入层可以由一些无线网卡、AP 和二层交换机等性价比高的设备组成，对于无线局域网 WLAN 用户，用户终端通过无线网卡和无线接入点 AP 完成用户接入。

6.8.3 层次化网络结构设计案例

随着 Internet 的迅猛发展，学校教育手段也逐渐实现现代化，校园网已经成为一个借助信息化教育和管理手段的高水平的智能化、数字化的教学园区网络，最终实现统一网络管理、统一软件资源系统，并保证将来可扩展骨干网络节点互联带宽为 10Gbps，为师生提供高速接入网络，并实现网络远程教学、在线服务、教育资源共享等各种应用。

图 6-19 是中等职业学校校园网拓扑示例，使用了层次化的设计方法。下面就该层次化网络结构设计方案，分析如下：

（1）校园网采用 1000Mbps 做骨干，100Mbps 到桌面。

（2）网络中心机房设在办公楼里，办公楼分别与实训楼、教学楼相距 200m，两楼之间均用 10Gbps 光纤连接，提高了网络数据的传输能力。

（3）核心层配备了两台新一代多业务万兆核心路由交换机 RG-S6810E 设备端口聚合互联，提高了网络带宽，提供了核心设备间冗余备份，增强了网络的可靠性。

（4）网络中心机房内有 WWW 服务器、FTP 服务器、DNS 服务器、VOD 点播服务器、办公 OA 服务器等高性能的服务器组设备，设有基于 SAN 架构的磁盘阵列数据存储技术，用于帮助学校对校务、学籍、人事、网站等方面进行管理，实现学校的办公自动化，各系

统之间实现充分的资源共享，提高办公及管理效率。不仅提供学校网站发布、E-mail、Telnet、远程视频点播、远程电子阅览室、网上教学等简单服务，还包括如教学资料、教学课件、技能大赛培训常用的资料的 FTP 下载。

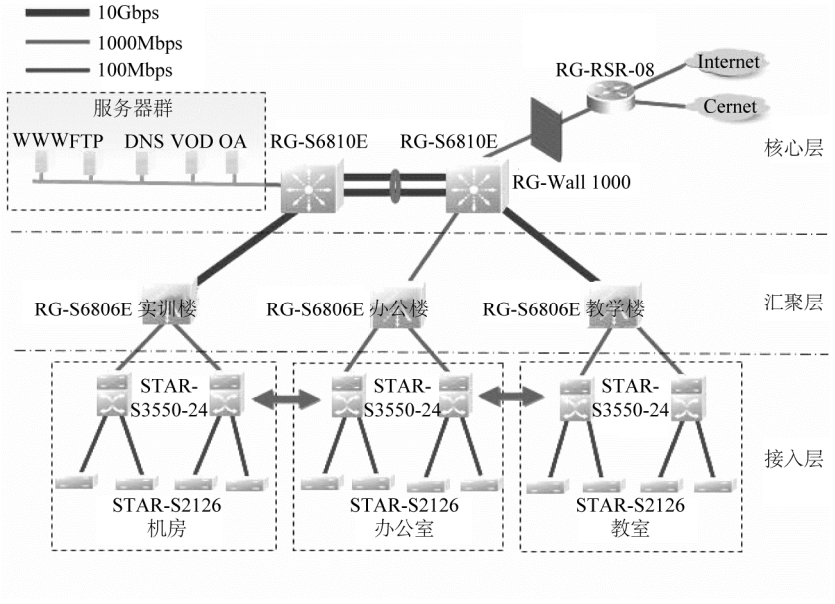


图 6-19　中职学校校园网拓扑示例

（5）校园网采用高性能、通用的骨干汇聚路由器（RG RSR-08）+防火墙（RG-Wall1000）结构进行 Internet 和 CERNER（中国教育和科研网）的接入，不仅提供了强大的数据处理能力、出口路由功能和 NAT 功能，而且具有强大的防范入侵和数据过滤功能，保证了内网通信安全，同时也为教师、学生、学生家长提供更好的信息交流和资源访问搭建了平台。

（6）汇聚层为办公楼、实训楼和教学楼各自的局域网络，均采用了锐捷 RG-S6806E 多业务万兆核心路由交换机，为接入层设备提供了强大的数据交换路由能力，实现了高速、高效、安全和智能的校园网新需求。

（7）接入层采用的是全千兆安全智能接入交换机 S3550-24 和 S2126，为行政办公室、各专业组办公室、各实验室机房、服务器组和学生教室提供了 VALN 环境，增强网络隔离、安全访问和实时管理功能。实验室机房各自划分的 VLAN 之间做到了不能互访，也不能访问其他区域，只能上网。专业组办公室各自划分的 VLAN 之间能做到互访，能上网和访问学生教室划分的 VLAN，但不能访问行政办公室划分的 VLAN。

（8）客户机均采用 TCP/IP 协议，分配 172.16.0.0 的内部私有 IP 地址，同时，配置接入层设备端口与客户机 MAC 地址绑定，以最大限度地减少 IP 地址的冲突和网络管理员的工作量。

习　题　6

一、填空题

1．路由器是工作在 OSI 参考模型_____层的数据包转发设备。

2．用户在任何模式提示符下输入_____，会显示当前模式下常用命令的列表及简单描述。

3．RIP 协议的网络直径不超过_____跳，适合于中小型网络。超_____跳时认为网络不可达。

4．ACL 分为_____和_____两种类型。

5．_____网络设备具有连接不同子网功能。

6．在配置 RG 系列路由器时，如果在特权模式下查看运行信息，使用_____命令。

7．路由器首次进行配置，一般利用_____端口。

8．联网的计算机可以用_____命令对路由器进行远程登录配置。

9．交换机端口安全接入某个特定设备，通常是利用端口与_____地址绑定来实现的。

10．层次化网络设计引入了_____、_____、_____三个关键层。

二、选择题

1．交换机如何知道将帧转发到哪个端口?（　　）

A．用 MAC 地址表　　B．用 ARP 地址表

C．读取源 ARP 地址　　D．读取源 MAC 地址

2．路由器配置了静态路由，如果收到的数据包中的目标地址与路由表中的所有条目都不匹配，路由器将把数据包（　　）。

A．保存　　B．丢弃

C．送往下一跳　　D．送往默认路由器

3．下列设备具有转发数据包的功能的是（　　）。

A．路由器　　B．网桥

C．集线器　　D．二层交换机

4．下列关于路由的描述中，较为接近动态路由的定义的是（　　）。

A．明确了目的地网络地址，但不能指定下一跳地址时采用的路由

B．由网络管理员手工设定的，明确指出了目的地网络和下一跳地址的路由

C．数据转发的路径没有明确指定，采用特定的算法来计算出一条最优的转发路径

D．以上说法都不正确

5．下面不是 VLAN 技术优点的是（　　）。

A．增加了组网的灵活性

B．可以减少碰撞的产生

C．提高了网络的安全性

D．在一台设备上阻隔广播，而不必额外的花销

6．路由器从用户模式进入特权模式的命令是（　　）。

A．router#enable

B．router>enable

C．router（config）#enable

D．router（config）>enable

7．以太网交换机是利用“端口/MAC 地址映射表”进行数据交换的。交换机实现动态建立和维护端口/MAC 地址映射表的方法是（　　）。

A．人工建立　　B．地址学习

C．进程　　D．轮询

8．基于距离矢量算法的路由协议是（　　）。

A．ICMP　　B．RIP

C．OSPF　　D．TCP

9．动态路由基于路由协议，（　　）并维护路由表。

A．手工指定　　B．自动生成

C．任意生成　　D．固定不变

10．一个 VLAN 可以看做一个（　　）。

A．冲突域　　B．广播域

C．管理域　　D．阻塞域

11．要禁止内网中 IP 地址为 198.168.46.8 的 PC 访问外网，正确的 ACL 规则是（　　）。

A．access-list 1 permit ip 192.168.46.0 0.0.0.255 any
access-list 1 deny ip host 198.168.46.8 any

B．access-list 1 permit ip host 198.168.46.8 any
access-list 1 deny ip 192.168.46.0 0.0.0.255 any

C．access-list 1 deny ip 192.168.46.0 0.0.0.255 any
access-list 1 permit ip host 198.168.46.8 any

D．access-list 1 deny ip host 198.168.46.8 any
access-list 1 permit ip 192.168.46.0 0.0.0.255 any

12．以太网中使用生成树算法的目的是（　　）。

A．避免来自同一端口的路由更新数据包转发到本端口

B．生成无环路的逻辑树形结构，尽最大可能在局域网段之间建立一条通路

C．在每一个局域网段之间建立一条路径

D．确保数据信息到达每一个节点

13．如图 6-20 所示，左面路由器中应该添加的由 192.168.10.1 到 192.168.30.1 的静态路由的是（　　）。

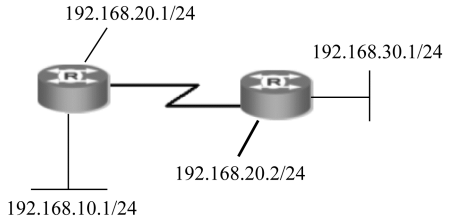


图 6-20

A．Router（config）#ip route 192.168.30.0 255.255.255.0 192.168.20.2

B．Router（config）#ip route 192.168.30.0 255.255.255.0 192.168.20.0

C．Router（config-if）#ip route 192.168.30.1 255.255.255.0 192.168.20.2

D．Router（config-if）#ip route 192.168.30.0 255.255.255.0 192.168.20.2

14．要想拒绝主机 192.168.100.3/24 访问服务器 201.10.182.10/24 的 WWW 服务，下面的访问控制列表配置及其模式均正确的是（　　）。

A．Router#ip access-list 101 deny tcp 192.168.100.3 0.0.0.255 201.10.182.10 0.0.0.255 eq 80

B．Router（config）#ip access-list 10 deny tcp 192.168.100.30 0.0.0.255 201.10.182.10 0.0.0.255 eq 80

C．Router（config-serial1/0）#ip access-list 10 deny tcp 192.168.100.3 0.0.0.255 201.10.182.10 0.0.0.255 eq 80

D．Router（config）#ip access-list 101 deny tcp 192.168.100.3 0.0.0.255 201.10.182.10 0.0.0.255 eq 80

15．关于链路聚合的说法不正确的是（　　）。

A．在一个链路聚合组里，每个端口必须工作在全双工模式下

B．在一个链路聚合组里，每个端口必须属于同一个 VLAN

C．在一个链路聚合组里，每条链路的属性必须和第一条链路的属性一致

D．在一个链路聚合组里，链路之间具有互相备份的功能

16．如果企业内部需要接入 Internet 的用户一共有 400 个，但该企业只申请到一个 C 类的合法 IP 地址，则应该使用（　　）方式实现。

A．静态 NAT　　B．动态 NAT

C．Port NAT　　D．以上都不对

17．以下对于默认路由描述不正确的是（　　）。

A．默认路由是优先被使用的路由

B．默认路由是最后一条被使用的路由

C．默认路由是一种特殊的静态路由

D．默认路由是一般在自治系统接入 Internet 的边界路由器上通常配置的路由

18．在接口应用 ACL，下面命令正确的是（　　）。

A．permit access-list 101 out

B．ip access-group 101 out

C．ip access-list f 0/0　out

D．ip access-class 101　out

19．如图 6-21 所示环境，如果对于整个网络配置 OSPF 协议（area 1），使其相互实现互通，则下列 RG 系列路由器的配置正确的是（　　）。

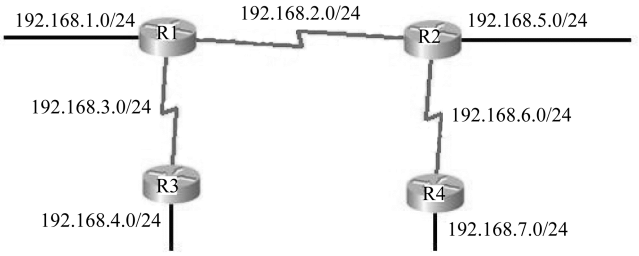


图 6-21

A．R1（config）#router ospf 100
R1（config）#network 192.168.1.0 255.255.255.0 area 1
R1（config）#network 192.168.2.0 255.255.255.0 area 1
R1（config）#network 192.168.3.0 255.255.255.0 area 1

B．R2（config）#router ospf 200
R2network 192.168.5.0 255.255.255.0 area 1
R2（config）#network 192.168.6.0 255.255.255.0 area

C．R3（config）#router ospf 70
R3（config）#network 192.168.3.0 0.0.0.255 area 1
R3（config）#network 192.168.4.0 0.0.0.255 area 1
R3（config）#network 192.168.5.0 0.0.0.255 area 1

D．R4（config）#router ospf　2
R4（config）#network 192.168.5.1 255.255.255.0 area 1
R4（config）#network 192.168.7.1 255.255.255.0 area 1

20．在 RG-S3760 中，下面命令可以把一个端口加入一个链路聚合组 10 中的是（　　）。

A．RG-S3760（config）#port-group 10
B．RG-S3760（config-if）#port-group
C．RG-S3760（config-if）#port-group 10
D．RG-S3760#port-group 10

三、简答题

1．VLAN 间路由在三层交换机上是如何实现的？

2．若一组交换机端口要组成汇聚端口，它们的哪些属性必须相同？

3．下面是某交换机的配置信息，解释部分语句的含义。

switch>enable _____

switch#config t _____

switch（config）#hostname student _____

student（config）#interface vlan 1 _____

student（config-if）#ip address 192.168.12.1 255.255.255.0

student（config-if）#exit _____

student（config）#interface f 0/2 _____

student（config-if）#speed 100 _____

student（config-if）#duplex full _____

student（config-if）#no shutdown _____

student（config-if）#exit

student（config）#vlan 10 _____

student（config-vlan）#exit

student（config）#interface vlan 10 _____

student（config-if）#ip address 192.168.13.1 255.255.255.0

student（config-if）#exit

student（config）#interface range f 0/11-20 _____

student（config-if）#switchport access vlan 10 _____

student（config-if）#exit

student（config）interface f 0/24

student（config-if）#switchport mode trunk _____

student（config-if）#end _____

student#show vlan _____

student#show run _____

student#write _____

4．如图 6-22 所示，如果路由器 A 要访问路由器 D 的 10.1.5.1/16 地址，请分别写出路由器 A、B、D 所要配置的静态路由、RIP 路由和 OSPF 路由。

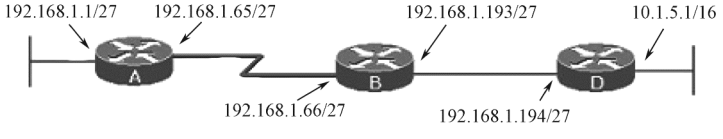


图6-22

5．创建拒绝来自 192.168.4.0 去往 192.168.3.0 的 FTP 流量的 ACL，允许其他流量能够访问，应用到接口 Fa 0/0 的出方向。

综 合 实 训

实训 1　双绞线线缆的制作

一、实训目的

1．了解双绞线的分类及应用场合。
2．掌握非屏蔽双绞线直通线缆与交叉线缆的制作方法。
3．掌握线缆测试仪的使用方法。

二、实训内容

1．分别制作双绞线直通、交叉线缆。
2．利用测试仪测试线缆的连通性。

三、实训条件

超 5 类非屏蔽双绞线缆若干段（长约 1.5m），RJ-45 水晶头、线标、护套若干个，RJ-45 线缆测试仪，压线钳

四、实验原理

（1）双绞线是由两对或更多对颜色各异的绝缘金属线组成的，每对金属线相互缠绕作为一条通信线路，可有效降低信号干扰程度。局域网中常用到的是非屏蔽超 5 类和 6 类双绞线。

（2）双绞线分为直通线和交叉线两种。

直通线就是水晶头两端按照同一标准连接，在工程中使用较多的是 EIA/TIA 586B 标准，主要用于计算机到交换机、交换机到交换机的连接。线序如下：

线　序	1	2	3	4	5	6	7	8
EIA/TIA568 B	白橙	橙	白绿	蓝	白蓝	绿	白棕	棕
EIA/TIA568B	白橙	橙	白绿	蓝	白蓝	绿	白棕	棕

交叉线是一端按照 EIA/TIA586B 标准、另一端按照 EIA/TIA586A 标准的接法，主要用于两台计算机直接连接。线序如下：

线　序	1	2	3	4	5	6	7	8
EIA/TIA568 B	白橙	橙	白绿	蓝	白蓝	绿	白棕	棕
EIA/TIA568 A	白绿	绿	白橙	蓝	白蓝	橙	白棕	棕

五、实训过程

任务 1　制作直通线缆

（1）穿线标、护套

线标与护套各自的作用是_____。

（2）剥线

利用压线钳将双绞线的外皮除去_____cm 左右，将划开的外保护套管剥去（旋转、向外抽）。

难点：在剥双绞线外皮时，手握压线钳用力要适当，否则损伤内部线芯，甚至会把线芯剪断。

（3）理线

通常按_____线序标准将 8 根导线平坦整齐地平行排列，导线间不留空隙，将裸露出的双绞线用压线钳剪下只剩约_____cm 的长度，一定要剪得很整齐。

思考：剪齐后裸露出的双绞线过长或过短有什么问题？

（4）插线

左手拿水晶头将弹簧卡方向_____，然后右手将正确排列的双绞线平行插入水晶头中，一定要将各条芯线都插到_____，与水晶头的_____完全接触，双绞线的外保护层应能够在 RJ-45 插头内的凹陷处被压实。

思考：为什么双绞线的外保护层也要插在水晶头里面？

（5）压线

在确认一切都正确后，将 RJ-45 插头放入_____的压头槽内，双手紧握压线钳的手柄，用力压制。

思考：出现双绞线芯与水晶头针脚接触不好的原因。

（6）重复（1）～（5）步，制作另一端 RJ-45 接头。

（7）测线

将双绞线两端分别接到测线仪的主控端和测线端，打开测线仪开关，则测线仪的指示灯按_____顺序依次绿色闪亮。

如果指示灯闪亮的顺序不一样，则说明_____；如果指示灯中有的呈现绿灯、有的不亮，则说明_____。

任务 2　制作交叉线缆

（1）交叉线的两端分别按照_____标准和_____标准制作。需将_____线与_____线，_____线与_____线位置对调即可。

（2）参照直通线的做法制作一根交叉线缆。

（3）测线。

将双绞线两端分别接到测线仪的主控端和测线端，打开测线仪开关， 则主控端的指示灯按_____顺序绿色闪亮，测线端指示灯按_____顺序绿色闪亮。

如果测线端第 1、3 个灯不亮，表示_____，应怎样处理_____。

六、实训小结

通过本次实训，你掌握了哪些技能？

实训 2　IP 地址与子网掩码

一、实训目的

1．理解 IP 地址及子网掩码的概念。
2．掌握 IP 在网络中的作用、格式及分配原则。
3．理解子网掩码在网络中的作用。

二、实训内容

1．IP 地址的设置与分配原则。
2．子网掩码的基本设置方法。

三、实训条件

4 台安装 Windows XP 操作系统的计算机，且已组建小型对等网络。

四、实训原理

1．IP 地址

IP 地址用来标识网络中的通信实体，由 32 位二进制数组成。为方便使用，采用“点分十进制表示法”表示 IP 地址：由四段构成的 32 比特的 IP 地址被直观地表示为 4 个以圆点隔开的十进制整数，其中，每一个整数对应一字节（8 比特为一字节称为一段）。对应的十进制取值为 0～255。

地址格式为：IP 地址=网络地址＋主机地址

或　　IP 地址=网络地址＋子网地址＋主机地址

网络地址是由 Internet 权力机构（InterNIC）统一分配的，目的是保证网络地址的全球唯一性。主机地址是由各个网络的系统管理员分配的。因此，网络地址的唯一性与网络内主机地址的唯一性确保了 IP 地址的全球唯一性。

2．IP 地址的分类

IP 地址根据需要被分为 5 个大类：A、B、C、D、E 类。A 类地址最高位为 0，紧跟的 7 位表示网络号，余 24 位表示主机号，总共允许有 126 个网络。B 类地址最高两位总被置于二进制的 10，允许有 16384 个网络。C 类地址高三位被置为二进制的 110，允许大约 200 万个网络。D 类地址被用于多路广播组用户，高四位总被置为二进制的 1110，余下的位用于标明客户机所属的组。E 类地址是一种仅供试验的地址。

3．私有 IP 地址

私有地址属于非注册地址，不在公网上分配，专门为组织机构内部使用。其地址范围如下：

A 类 10.0.0.0～10.255.255.255

B 类 172.16.0.0～172.31.255.255

C 类 192.168.0.0～192.168.255.255

4．子网掩码

子网掩码用来指明 IP 地址中网络和主机地址部分，是判断任意两台计算机的 IP 地址是否属于同一广播域的依据。子网掩码不能单独存在，它必须结合 IP 地址一起使用。与 IP 地址相同，子网掩码的长度也是 32 位，前一部分用连续的“1”标识网络地址，后一部分用连续的“0”标识主机地址。默认的子网掩码为：A 类 255.0.0.0，B 类 255.255.0.0，C 类 255.255.255.0。

五、实训过程

1．在 PC1 输入 IP 地址 127.1.5.2，观察能否设置，分析原因。

2．在 PC2 输入 IP 地址 192.168.1.255，观察能否设置，分析原因。

3．在 PC3 输入 IP 地址 192.168.1.0，观察能否设置，分析原因。

4．在 PC4 输入 IP 地址 10.0.0.1，观察能否设置，子网掩码默认是什么。

5．设置 4 台计算机的 IP 地址和子网掩码如下：

	PC1	PC2	PC3	PC4
IP 地址	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.4
子网掩码	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

（1）在 PC1 分别用“ping”命令测试 PC2、PC3、PC4 机器，观察能否连通。

（2）将 PC2 的 IP 地址改为 192.168.1.3，观察系统会给出什么提示，分析原因。

（3）将 PC2 的 IP 地址改为 192.168.2.2，观察与其他计算机能否连通，分析原因。

（4）将 PC3 子网掩码改为 255.255.0.0，观察与其他计算机能否连通，分析原因。

6．设置 4 台计算机的 IP 地址和子网掩码如下：

	PC1	PC2	PC3	PC4
IP 地址	192.168.10.51	192.168.10.60	192.168.10.66	192.168.10.125
子网掩码	255.255.255.240	255.255.255.240	255.255.255.240	255.255.255.240

（1）本网络共分为多少个子网？每个子网最多可有多少台计算机？

（2）这 4 个 IP 地址涉及几个子网？相互间用“ping”命令测试连通，哪些计算机连通、哪些不通？分析原因。

（3）如将 PC3 的 IP 地址改为 192.168.10.62，此时它可与哪些计算机连通？说明原因。

（4）PC4 所在子网的广播地址是什么？子网号是什么？

7．设置 4 台计算机的 IP 地址和子网掩码如下：

	PC1	PC2	PC3	PC4
IP 地址	192.168.8.8	192.168.9.8	192.168.10.8	192.168.11.8
子网掩码	255.255.252.0	255.255.252.0	255.255.252.0	255.255.252.0

测试 4 台计算机之间能否正常通信，说明原因。

六、实训小结

通过本次实训，你掌握了哪些技能？

实训 3　组建对等网络

一、实验目的

1．理解对等网的概念。
2．掌握对等网的规划与配置。
3．掌握网络连通测试方法。

二、实验内容

1．对等网的安装与配置。
2．网络连通性的测试。

三、实训条件

1．安装有 Windows XP 操作系统的计算机 3 台。
2．100Mbps PCI 接口网卡 3 块。

3．多端口交换机 1 台。

4．直通双绞线若干根。

四、实训原理

1．对等网络

对等网也称为工作组网，其特点是对等性，即网络中计算机功能相似，地位相同，无专用服务器。每台计算机相对网络中其他的计算机而言，既是服务器又是客户机，相互共享网络资源。

2．对等网的规划

（1）规划拓扑结构

对等网中由于包含计算机数量较少，通常采用星型拓扑结构。

（2）计算机名和工作组规划

在对等网中计算机名不能重复，否则无法正确识别计算机。同一对等网中的计算机应属于同一工作组，即工作组名相同。但计算机处于不同工作组中，并不影响相互间的访问。

（3）IP 地址的规划

同一对等网中各计算机 IP 地址中主机地址不能相同，但网络地址必须相同，通常使用私有 IP 地址。

3．网络连通性测试

通过系统提供的 ping 应用程序检查网络是否通畅或者网络连接速度。命令格式：ping IP 地址或主机名

五、实训过程

1．设计拓扑结构

根据提供的硬件设备，规划设计一个小型对等网络，请设计出该网络的拓扑结构。

2．安装网卡及驱动程序

（1）关闭机箱电源，将网卡插入主板上一个空闲 PCI 插槽内，将网卡与机箱接口处的螺钉固定好，防止出现短路。

（2）开机启动 Windows XP 系统，自动检测到新安装的网卡，按照提示安装网卡驱动程序。

（3）查看网卡配置信息和 MAC 地址

① 在“网络连接”中，用鼠标右键单击“本地连接”图标，在弹出的快捷菜单中选择“状态”选项，打开“本地连接状态”对话框，选择“支持”选项卡查看。

② 在命令行模式中输入“ipconfig/all”查看相关信息。

3．小型对等网络硬件连接

（1）将直通网线一头插到交换机 RJ-45 插槽内，另一头插到 PC1 的网卡 RJ-45 插槽。其他两台机器接法相同。

（2）开机后，观察计算机网卡与交换机相对应端口指示灯变化情况，说明其代表的含义。

4．IP 地址的规划与配置

（1）IP 地址规划

主 机 名	IP 地址	子 网 掩 码	默 认 网 关
PC1	192.168.1.3	255.255.255.0	192.168.1.1
PC2	192.168.1.4	255.255.255.0	192.168.1.1
PC3	192.168.1.5	255.255.255.0	192.168.1.1

（2）配置 IP 地址

根据已规划的 IP 地址，分别在本机的 TCP/IP 协议属性对话框内设置 IP 地址、子网掩码、默认网关等信息。

5．计算机名和工作组的规划与设置

（1）分别在本机的计算机属性对话框内设置计算机名为 PC1、PC2、PC3，工作组名为 WORKGROUP。

（2）如果两台计算机重名会出现什么问题？工作组名不同，计算机间是否可以正常互访？

6．网络连通性测试

（1）测试本机网卡是否正常运行（ping 本机 IP 地址）

观察屏幕显示结果，如测试不通过，判断故障原因。

（2）测试本地 TCP/IP 协议栈是否正常

输入命令 ping 127.0.0.1，观察屏幕显示结果，判断 TCP/IP 协议栈是否正常工作。

（3）分别测试 PC1 与 PC2、PC1 与 PC3 之间的连通性，观察网络通信是否正常。如果 PC1 与 PC2 测试不通，判断故障原因并解决。

六、实训小结

通过本次实训，你掌握了哪些技能？

实训 4　交换机的基本配置

一、实训目的

掌握交换机的管理特性，学会配置交换机支持 Telnet 操作的相关语句。

二、实训背景

假设某公司的网络管理员在设备机房第一次对交换机进行了初次配置后，他希望以后在办公室或出差时也可以通过网络对设备进行远程管理，现要在交换机上做适当的配置，就可实现上述功能。

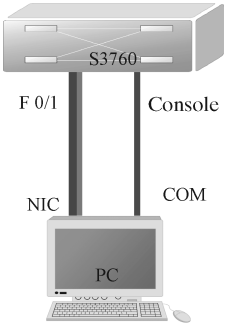
本实训以 S3760-48 交换机为例，交换机命名为 S3760。通过反转线将 PC 的串口（COM）和交换机的控制（Console）端口连接，通过交叉线将 PC 的网卡（NIC）端口和交换机的 F0/1 端口连接。假设这台 PC 的 IP 地址为 192.168.1.10/24，配置交换机的管理 IP 地址为 192.168.1.200/24。

三、实训条件

（1）S3760-48 交换机 1 台。
（2）PC 1 台。
（3）交叉线 1 根。
（4）反转线 1 根。

四、实训拓扑

拓扑结构如下图所示。



五、实训过程

（1）认识各线缆、PC 的 COM 端口、交换机端口和 Console 端口，并按上图连接。
（2）配置 PC 的 IP 地址：192.168.1.10/24。
（3）在 PC 上打开超级终端窗口。
（4）打开交换机的电源，并在超级终端窗口中观察交换机启动过程。
（5）配置交换机的名称：S3760。
命令参考：

```
Red-Giant（config）#hostname S3760
```

（6）配置交换机的管理接口 IP 地址：192.168.1.200/24，并开启该接口。
命令参考：

```
S3760（config）#interface vlan 1
S3760（config-if）#ip address 192.168.1.200 255.255.255.0
S3760（config-if）#no shutdown
```

（7）验证交换机管理接口已经配置 IP 地址，并开启该接口。
命令参考：

```
S3760#show ip interface
S3760#show interface vlan 1
```

（8）配置交换机远程登录口令。
命令参考：

```
S3760（config）#line vty 0 4
S3760（config-line）#password ruijie
S3760（config-line）#login
```

（9）配置交换机特权模式口令。
命令参考：

```
S3760（config）#enable secret star
```

（10）查看交换机当前所有配置。
命令参考：

```
S3760#show running-config
```

（11）验证从 PC 通过网线远程登录到交换机上后可进入特权模式。
命令参考：

```
C：\>telnet 192.168.0.138
```

（12）保存在交换机上所做的所有配置。
命令参考：

```
S3760#write
或  S3760#copy running-config startup-config
```

六、实训小结

通过本次实训，你掌握了哪些技能？

实训 5　交换机端口隔离

一、实训目的

1．理解 VLAN 基本原理。
2．掌握同一交换机下的 VLAN 配置方法。
3．通过划分 Port VLAN 实现交换机端口的隔离。

二、实训背景

假设某公司办公楼的所有计算机都连接在同一个交换机下。公司经理要求普通员工不能访问经理的计算机和财务的计算机。假设你是该公司的网络管理员，现要你在交换机上做适当的配置，实现上述要求。

本实训以一台 S2126G 交换机为例，交换机命名为 S2126。通过直通线分别连接普通员

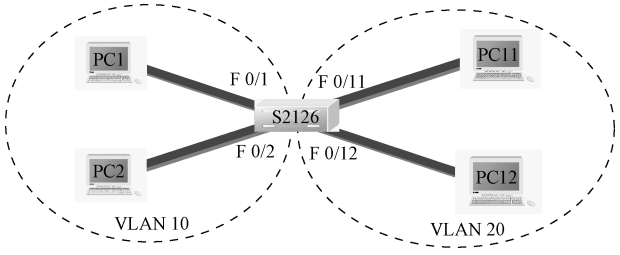
工的计算机 PC1 与交换机的 F 0/1 端口、普通员工的计算机 PC2 与交换机的 F 0/2 端口、经理的计算机 PC11 与交换机的 F 0/11 端口、财务的计算机 PC12 与交换机的 F 0/12 端口。假设 PC1 的 IP 地址为 192.168.1.1/24，PC2 的 IP 地址为 192.168.1.2/24，PC11 的 IP 地址为 192.168.1.11/24，PC12 的 IP 地址为 192.168.1.12/24。

三、实训条件

（1）S2126G 交换机 1 台。
（2）PC 4 台。
（3）直通线 4 根。
（4）反转线 1 根。

四、实训拓扑

拓扑结构如下图所示。



五、实训过程

（1）认识直通线、PC 的 NIC 端口、交换机各端口，并按上图连接。
（2）分别配置 PC1、PC2、P11、P12 的 IP 地址。
（3）利用 ping 命令验证各 PC 的互通性。
（4）通过一根反转线将交换机的 Console 端口与任意一台 PC 的 COM 端口连接，打开该 PC 的超级终端窗口，进行对交换机的配置。
（5）配置交换机的名称：S2126。
命令参考：

```
Red-Giant（config）#hostname S2126
```

（6）创建 VLAN10 和 VLAN20。
命令参考：

```
S2126（config）#vlan 10
S2126（config）#name ptyg
S2126（config）#vlan 20
```

```
S2126（config）#name jlcw
```

（7）验证 VLAN10 和 VLAN20 的创建。
命令参考：

```
S2126#show vlan
```

（8）将接口分配到 VLAN 中。
命令参考：

```
S2126（config）#interface fastethernet 0/1
S2126（config-if）#switchport access vlan 10
S2126（config）#interface fastethernet 0/2
S2126（config-if）#switchport access vlan 10
S2126（config）#interface range fastethernet 0/11-12
S2126（config-if-range）#switchport access vlan 20
```

注意：区分 VLAN10 和 VLAN20 接口分配的不同配置方法。
（9）再次验证 VLAN 及其分配的接口。
命令参考：

```
S2126#show vlan
```

注意：区分步骤（7）和（9）验证结果有何不同。
（10）再次利用 ping 命令验证各 PC 的互通性。
注意：区分步骤（3）和（10）验证结果有何不同。
（11）保存交换机 S2126 上所做的配置。

六、实训小结

通过本次实训，你掌握了哪些技能？

实训 6　跨交换机的 VLAN

一、实训目的

掌握如何在交换机上划分 Port VLAN 和配置 Trunk，实现跨交换机 VLAN 间的互访。

二、实训背景

假设某公司有二层楼，一楼有一个交换机，供一楼的业务部、技术部的计算机接入；二楼也有一个交换机，供二楼的业务部、技术部的计算机接入。公司经理要求两个部门的计算机不能互访。假设你是该公司的网络管理员，现要在交换机上做适当的配置，实现上述要求。

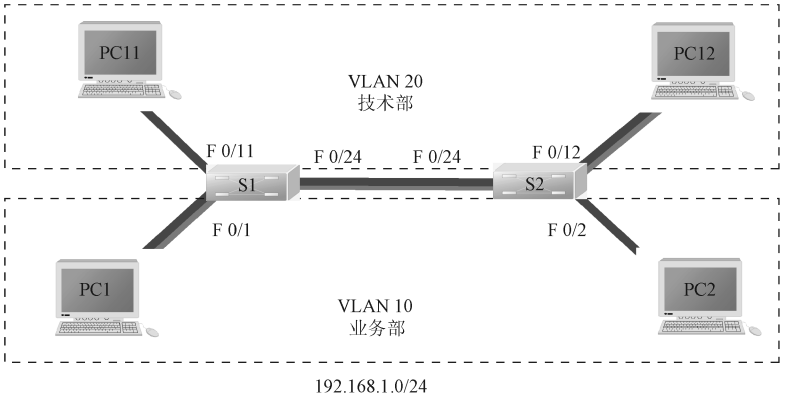
本实训以两台 S2126G 交换机为例，分别命名为 S1、S2。通过交叉线分别连接 S1、S2 的 F0/24 端口；业务部的计算机 PC1、PC2 分别与 S1 的 F0/1 端口、S2 的 F0/2 端口连接；技术部的计算机 PC11、PC12 分别与 S1 的 F0/11 端口、S2 的 F0/12 端口连接。假设 PC1 的 IP 地址为 192.168.1.1/24，PC2 的 IP 地址为 192.168.1.2/24，PC11 的 IP 地址为 192.168.1.11/24，PC12 的 IP 地址为 192.168.1.12/24。

三、实训条件

（1）S2126G 交换机 2 台。
（2）PC 4 台。
（3）双绞线 5 根。
（4）反转线 1 根。

四、实训拓扑

拓扑结构如下图所示。



五、实训过程

（1）认识各线缆、PCNIC 端口、交换机各端口，并按上图连接。
（2）分别配置 PC1、PC2、PC11、PC12 的 IP 地址。
（3）利用 ping 命令验证各 PC 的连通性。

（4）通过一根反转线分别将 S1、S2 的 Console 端口与任意一台 PC 的 COM 端口连接，打开该 PC 的超级终端窗口，进行对 S1、S2 的配置。

（5）分别配置两台交换机的名称：S1、S2。

（6）在 S1 和 S2 上分别创建业务部 VLAN10 和技术部 VLAN20。

命令参考：

```
S1（config）#vlan 10
S1（config）#name yewu
S1（config）#vlan 20
S1（config）#name jishu
S2（config）#vlan 10
S2（config）#name yewu
S2（config）#vlan 20
S2（config）#name jishu
```

（7）分别在 S1 和 S2 上验证 VLAN10 和 VLAN20 的创建。

命令参考：

```
S1#show vlan
S2#show vlan
```

（8）分别将 S1 和 S2 的接口分配到相应的 VLAN10、VLAN20 中。

命令参考：

```
S1（config）#interface fastethernet 0/1
S1（config-if）#switchport access vlan 10
S1（config）#interface fastethernet 0/11
S1（config-if）#switchport access vlan 20
S2（config）#interface fastethernet 0/2
S2（config-if）#switchport access vlan 10
S2（config）#interface fastethernet 0/12
S2（config-if）#switchport access vlan 20
```

（9）再次分别验证 S1 和 S2 中 VALN10、VLAN20 及其分配的接口。

注意：区分步骤（7）和（9）验证结果有何不同。

（10）再次利用 ping 命令验证各 PC 的互通性。

注意：区分步骤（3）和（10）验证结果有何不同。

（11）分别将 S1、S2 的接口 F 0/24 配置成 Trunk 模式。

命令参考：

```
S1（config）#interface fastethernet 0/24
S1（config-if）#switchport mode trunk
```

```
S2（config）#interface fastethernet 0/24
S2（config-if）#switchport mode trunk
```

（12）分别验证 S1、S2 接口 F 0/24 的模式。
命令参考：

```
S1#show interface fastethernet 0/24 switchport
S2#show interface fastethernet 0/24 switchport
```

（13）再次分别验证 S1 和 S2 中 VALN10、VLAN20 及其分配的接口。
注意：区分步骤（9）和（13）验证结果有何不同。
（14）再次利用 ping 命令验证各 PC 的互通性。
注意：区分步骤（10）和（14）的验证结果有何不同。
（15）分别保存两台交换机上所做的配置。

六、实训小结

通过本次实训，你掌握了哪些技能？

实训 7　VLAN 间的通信

一、实训目的

掌握如何在三层交换机上配置 SVI 接口，实现 VLAN 间的路由。

二、实训背景

假设某公司有二层楼，一楼有一个交换机，供一楼的业务部、技术部的计算机接入；二楼也有一个交换机，供二楼的业务部、技术部的计算机接入。公司经理要求两部门的计算机能互访。假设你是该公司的网络管理员，现要你在交换机上做适当的配置，实现上述要求。

本实训以两台 S2126G、S3550-24 交换机为例，分别命名为 S2126、S3550。通过交叉线分别连接 S2、S3 的 F0/24 端口；业务部的计算机 PC1、PC2 分别与 S2 的 F0/1 端口、S3 的 F0/2 端口连接；技术部的计算机 PC11、PC12 分别与 S2 的 F0/11 端口、S3 的 F0/12 端口连接。假设 PC1 的 IP 地址为 192.168.10.1/24，PC2 的 IP 地址为 192.168.10.2/24，PC11 的

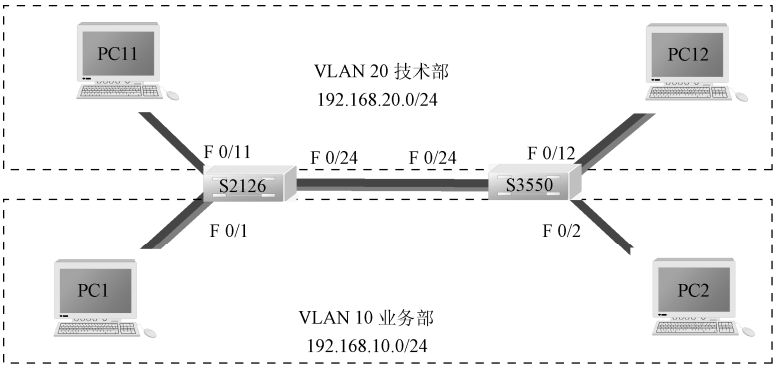
IP 地址为 192.168.20.11/24，PC12 的 IP 地址为 192.168.20.12/24。

三、实训条件

（1）S2126G 交换机 2 台。
（2）PC 4 台。
（3）双绞线 5 根。
（4）反转线 1 根。

四、实训拓扑

拓扑结构如下图所示。



五、实训过程

（1）认识各线缆、PC 的 NIC 端口、交换机各端口，并按上图连接。
（2）分别配置 PC1、PC2、PC11、PC12 的 IP 地址。
（3）利用 ping 命令验证各 PC 的连通性。
（4）通过一根反转线分别将 S2126、S3550 的 Console 端口与任意一台 PC 的 COM 端口连接，打开该 PC 的超级终端窗口，进行对 S2126、S3550 的配置。
（5）分别配置两台交换机的名称：S2126、S3550。
（6）在 S2126 和 S3550 上分别创建业务部 VLAN10 和技术部 VLAN20。
命令参考：

```
S2126（config）#vlan 10
S2126（config）#name yewu
S2126（config）#vlan 20
S2126（config）#name jishu
S3550（config）#vlan 10
S3550（config）#name yewu
```

```
S3550（config）#vlan 20
S3550（config）#name jishu
```

（7）分别验证 S2126 和 S3550 中 VLAN10、VLAN20 的创建。
命令参考：

```
S2126#show vlan
S3550#show vlan
```

（8）分别将 S2126 和 S3550 的接口分配到相应的 VLAN10、VLAN20 中。
命令参考：

```
S2126（config）#interface fastethernet 0/1
S2126（config-if）#switchport access vlan 10
S2126（config）#interface fastethernet 0/11
S2126（config-if）#switchport access vlan 20
S3550（config）#interface fastethernet 0/2
S3550（config-if）#switchport access vlan 10
S3550（config）#interface fastethernet 0/12
S3550（config-if）#switchport access vlan 20
```

（9）分别验证 S2126 和 S3550 中 VLAN10、VLAN20 及其分配的接口。
注意：区分步骤（7）和（9）验证结果有何不同。
（10）再次利用 ping 命令验证各 PC 的互通性。
注意：区分步骤（3）和（10）验证结果有何不同。
（11）分别将 S2126、S3550 的接口 F 0/24 配置成 Trunk 模式。
命令参考：

```
S2126（config）#interface fastethernet 0/24
S2126（config-if）#switchport mode trunk
S3550（config）#interface fastethernet 0/24
S3550（config-if）#switchport mode trunk
```

（12）分别验证查看 S2126、S3550 接口 F0/24 的模式。
命令参考：

```
S2126#show interface fastethernet 0/24 switchport
S3550#show interface fastethernet 0/24 switchport
```

（13）再次分别验证查看 S2126 和 S3550 中 VLAN10、VLAN20 及其分配的接口。
注意：区分步骤（9）和（13）验证结果有何不同。
（14）再次利用 ping 命令验证各 PC 的互通性。
注意：区分步骤（10）和（14）的验证结果有何不同。

（15）在三层交换机 S3550 中分别配置 VLAN10 和 VLAN20 的 SVI 接口 IP 地址并开启激活。

命令参考：

```
S3550（config）#interface vlan 10
S3550（config-if）#ip address 192.168.10.245 255.255.255.0
S3550（config-if）#no shutdown
S3550（config）#interface vlan 20
S3550（config-if）#ip address 192.168.20.245 255.255.255.0
S3550（config-if）#no shutdown
```

（16）配置 PC1 和 PC2 的网关为 192.168.10.254；PC11 和 PC12 的网关为 192.168.20.254。

注意：需要配置各 PC 的网关为相应 VLAN 的 SVI 接口地址。

（17）再次利用 ping 命令验证各 PC 的互通性。

注意：区分步骤（14）和（17）的验证结果有何不同。

（18）查看 S3550 的路由表。

命令参考：

```
S3550#show ip route
```

（19）分别保存两台交换机上所做的配置。

六、实训小结

通过本次实训，你掌握了哪些技能？

实训 8　聚合端口和快速生成树协议 RSTP

一、实训目的

1．理解聚合端口和生成树协议 RSTP 的作用和工作原理。

2．掌握如何在交换机上配置聚合端口和生成树协议。

二、实训背景

假设某公司有两台交换机，一台交换机连接各部门服务器，另外一台交换机连接各部门员工的 PC。每个部分的员工要频繁访问自己部门的服务器，为了提高交换机之间的传输带宽，并实现链路冗余备份，同时防止广播风暴的产生，为此该公司的网络管理员在两台交换机之间采用两根网线互联，并将相应的两个端口聚合为一个逻辑端口，现要在交换机上做适当的配置来实现上述功能。

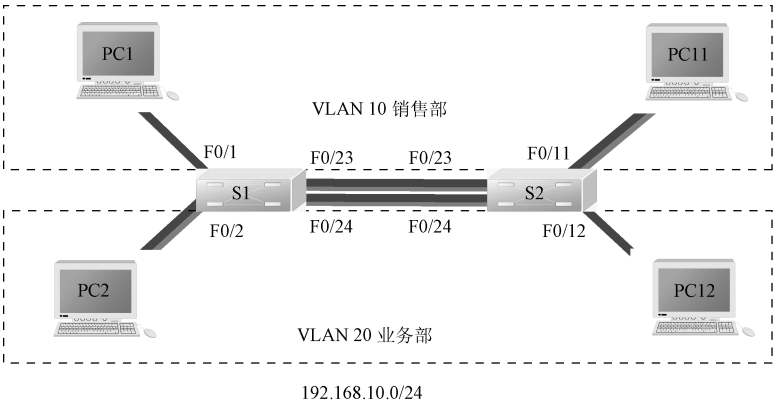
本实训以两台 S2126G 交换机为例，分别命名为 S1、S2。通过两根交叉线分别连接 S1、S2 的 F 0/23、F 0/24 端口；销售部的服务器 PC1 连接 S1 的 F 0/1 端口、员工计算机 PC11 连接 S2 的 F 0/11 端口；业务部的服务器 PC2 连接 S1 的 F 0/2 端口、员工计算机 PC12 连接 S2 的 F 0/12 端口。假设 PC1 的 IP 地址为 192.168.10.1/24，PC2 的 IP 地址为 192.168.10.2/24，PC11 的 IP 地址为 192.168.10.11/24，PC12 的 IP 地址为 192.168.10.12/24。

三、实训条件

（1）S2126G 交换机 2 台。
（2）PC4 台。
（3）双绞线 6 根。
（4）反转线 1 根。

四、实训拓扑

拓扑结构如下图所示。



五、实训过程

（1）认识各线缆、PC 的 NIC 端口、交换机各端口，并按上图连接。
（2）分别配置 PC1、PC2、PC11、PC12 的 IP 地址。

（3）利用 ping 命令验证各 PC 的连通性。

（4）通过一根反转线分别将 S1、S2 的 Console 端口与任意一台 PC 的 COM 端口连接，打开该 PC 的超级终端窗口，进行对 S1、S2 的配置。

（5）分别配置两台交换机的名称：S1、S2。

（6）在 S1 和 S2 上分别创建销售部 VLAN10 和业务部 VLAN20。

命令参考：

```
S1（config）#vlan 10
S1（config）#name xiaoshou
S1（config）#vlan 20
S1（config）#name yewu
S2（config）#vlan 10
S2（config）#name xiaoshou
S2（config）#vlan 20
S2（config）#name yewu
```

（7）分别将 S1 和 S2 的接口分配到相应的 VLAN10、VLAN20 中。

命令参考：

```
S1（config）#interface fastethernet 0/1
S1（config-if）#switchport access vlan 10
S1（config）#interface fastethernet 0/2
S1（config-if）#switchport access vlan 20
S2（config）#interface fastethernet 0/11
S2（config-if）#switchport access vlan 10
S2（config）#interface fastethernet 0/12
S2（config-if）#switchport access vlan 20
```

（8）分别验证 S1 和 S2 中 VLAN10、VLAN20 的创建及其分配的接口。

命令参考：

```
S1#show vlan
S2#show vlan
```

（9）在 S1 和 S2 上分别创建一个聚合端口，并把相应以太网端口加入此聚合端口中。

命令参考：

```
S1（config）#interface aggregatePort 1
S1（config-if）#switchport mode trunk
S1（config）#interface range fastethernet 0/23-24
S1（config-if-range）#port-group 1
S2（config）#interface aggregatePort 1
```

```
S2（config-if）#switchport mode trunk
S2（config）#interface range fastEthernet 0/23-24
S2（config-if-range）#port-group 1
```

注意：只有同类型端口才能聚合为一个端口。

（10）分别验证 S1 和 S2 聚合端口的创建。

命令参考：

```
S1#show aggregatePort 1 summary
S2#show aggregatePort 1 summary
```

（11）验证当交换机之间的一条链路断开时，PC1 与 PC11、PC2 与 PC12 仍能互相通信。

命令参考：

在 PC1 中，输入 C:\ping 192.168.10.11 -t

在 PC2 中，输入 C:\ping 192.168.10.12 -t

（12）分别开启两台交换机的生成树协议，设置其模式为 RSTP 协议。

命令参考：

```
S1（config）#spanning-tree
S1（config）#spanning-tree mode rstp
S2（config）#spanning-tree
S2（config）#spanning-tree mode rstp
```

注意：锐捷交换机默认是关闭 spanning-tree 的，因此，如果网络在物理上存在环路，则必须手工开启 spanning-tree。另外，锐捷全系列交换机生成树协议模式默认为 MSTP 协议。

（13）分别验证查看两台交换机上的生成树协议已经开启，其模式为 RSTP。

命令参考：

```
S1#show spanning-tree
S1#show spanning-tree interface fastethernet 0/23
S1#show spanning-tree interface fastethernet 0/24
S2#show spanning-tree
S2#show spanning-tree interface fastethernet 0/23
S2#show spanning-tree interface fastethernet 0/24
```

（14）设置交换机的优先级。

命令参考：

```
S1（config）#spanning-tree priority 4096
S2（config）#spanning-tree priority32768
```

注意：设置 S1 的优先级为 4096，S2 的优先级为 32768，因此数值最小的 S1 为根交换机（也称为根桥）。

（15）再次分别综合验证两台交换机端口 F0/23 和 F0/24 的状态。
（16）分别保存两台交换机上所做的配置。

六、实训小结

通过本次实训，你掌握了哪些技能？

实训 9　路由器的基本配置

一、实训目的

掌握路由器的管理特性，学会配置路由器支持 Telnet 操作的相关语句。

二、实训背景

假设某公司的网络管理员在设备机房第一次对路由器进行了初次配置后，他希望以后在办公室或出差时也可以通过网络对设备进行远程管理，现要在路由器上做适当的配置，就可实现上述功能。

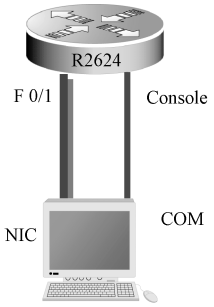
本实训以一台 R2624 路由器为例，路由器命名为 R2624。通过反转线将 PC 的串口（COM）和路由器的控制（Console）端口连接，通过交叉线将 PC 的网卡（NIC）端口和路由器的 F0/1 端口连接。假设这台 PC 的 IP 地址为 192.168.1.10/24，配置路由器 F0/1 端口的 IP 地址为 192.168.1.200/24。

三、实训条件

（1）R2624 路由器 1 台。
（2）PC 1 台。
（3）交叉线 1 根。
（4）反转线 1 根。

四、实训拓扑

拓扑结构如下图所示。



五、实训过程

（1）认识各线缆、PC 的 COM 端口、路由器各端口和 Console 端口，并按上图连接。
（2）配置 PC 的 IP 地址：192.168.1.10/24。
（3）在 PC 上打开超级终端窗口。
（4）打开路由器的电源，并在超级终端窗口中观察路由器启动过程。
（5）配置路由器的名称：R2624。
命令参考：

```
Red-Giant（config）#hostname R2624
```

（6）配置路由器 F 0/1 端口的 IP 地址：192.168.1.200/24，并开启该端口。
命令参考：

```
R2624（config）#interface f0/1
R2624（config-if）#ip address 192.168.1.200 255.255.255.0
R2624（config-if）#no shutdown
```

（7）验证路由器端口已经配置 IP 地址，并开启该端口。
命令参考：

```
R2624#show ip interface f0/1
```

或

```
R2624#show interface brief
```

（8）配置路由器远程登录口令。
命令参考：

```
R2624（config）#line vty 0 4
R2624（config-line）#login
R2624（config-line）#password ruijie
```

（9）配置路由器特权模式口令。
命令参考：

```
R2624（config）#enable password star
```

或

```
R2624（config）#enable secret star
```

（10）查看路由器当前所有配置。
命令参考：

```
R2624#show running-config
```

（11）验证从 PC 通过网线远程登录到路由器上后可进入特权模式。
命令参考：

```
C:\>telnet 192.168.0.138
```

（12）保存在路由器上所做的所有配置。
命令参考：

```
R2624#write
```

或

```
R2624#copy running-config startup-config
```

（13）查看路由器已保存的所有配置。
命令参考：

```
R2624#show startup-config
```

六、实训小结

通过本次实训，想一想与实训 4 有什么不同，你又掌握了哪些技能？

实训 10　静态路由

一、实训目的

1．理解静态路由工作原理。
2．掌握如何在路由器上配置静态路由实现网络的互通。

二、实训背景

假设某学校有东西两个校区，每个校区使用一台路由器连接一个局域网。假设你是该校的网络管理员，现要在两台路由器上配置静态路由，实现东西两个校区网络互通。

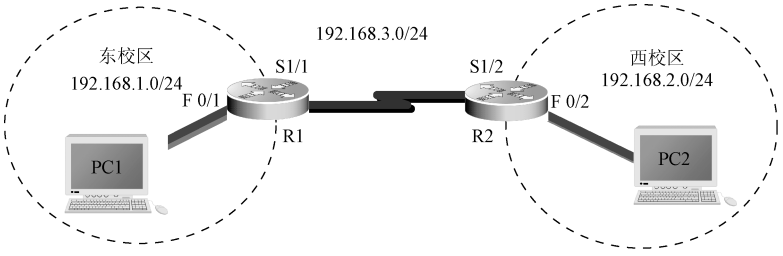
本实训以两台 R2624 路由器为例，分别命名为 R1、R2，通过串口以 V.35 DCE/DTE 电缆连接；通过交叉线分别将 PC1 和 R1 的 F0/1 端口、PC2 和 R2 的 F0/2 端口连接。假设 PC1 的 IP 地址为 192.168.1.10/24，PC2 的 IP 地址为 192.168.2.20/24；R1 的 S1/1 端口的 IP 地址为 192.168.3.1/24，F0/1 端口的 IP 地址为 192.168.1.1/24；R2 的 S1/2 端口的 IP 地址为 192.168.3.2/24，F0/2 端口的 IP 地址为 192.168.2.1/24。

三、实训条件

（1）R2624 路由器 2 台。
（2）PC2 台。
（3）V.35 DCE/DTE 电缆 1 根。
（4）交叉线 2 根。
（5）反转线 1 根。

四、实训拓扑

拓扑结构如下图所示。



五、实训教程

（1）认识各线缆、PC 的 COM 端口、路由器各端口和 Console 端口，并按上图连接。
（2）通过一根反转线分别将 R1、R2 的 Console 端口与任意一台 PC 的 COM 端口连接，打开该 PC 的超级终端窗口，进行对 R1、R2 的配置。
（3）分别配置两台路由器的名称：R1、R2。
（4）配置 R1 接口的 IP 地址和串口的时钟频率。
命令参考：

```
R1（config）#interface fastethernet 0/1
```

```
R1（config-if）#ip address 192.168.1.1 255.255.255.0
R1（config-if）#no shutdown
R1（config）#interface serial 1/1
R1（config-if）#clock rate 64000
R1（config-if）#ip address 192.168.3.1 255.255.255.0
R1（config-if）#no shutdown
```

注意：如果两台路由器通过串口直接互联，则必须在其中一端（DCE 端）设置时钟频率。

（5）验证 R1 接口配置。

命令参考：

```
R1#show ip interface brief
```

（6）配置 R1 的静态路由。

命令参考：

```
R1（config）#ip route 192.168.2.0 255.255.255.0 192.168.3.2
```

或

```
R1（config）#ip route 192.168.2.0 255.255.255.0 serial 1/1
```

（7）验证 R1 上的静态路由配置。

命令参考：

```
R1#show ip route
```

（8）配置 R2 接口的 IP 地址。

命令参考：

```
R2（config）#interface fastethernet 0/2
R2（config-if）#ip address 192.168.2.1 255.255.255.0
R2（config-if）#no shutdown
R2（config）#interface serial 1/2
R2（config-if）#ip address 192.168.3.2 255.255.255.0
R2（config-if）#no shutdown
```

注意：DTE 端不需要配置相应路由器接口的时钟频率。

（9）验证 R2 接口配置。

命令参考：

```
R2（config）#R1#show ip interface brief
```

（10）配置 R2 的静态路由。

命令参考：

```
R2（config）#ip route 192.168.1.0 255.255.255.0 192.168.3.1
```

或

```
R2（config）#ip route 192.168.2.0 255.255.255.0 serial 1/2
```

注意：这两条命令格式。

（11）验证 R2 上的静态路由配置。

命令参考：

```
R2#show ip route
```

（12）分别配置 PC1、PC2 的 IP 地址和网关地址。

注意：PC1 的网关地址为 R1 端口 F0/1 的 IP 地址，PC2 的网关地址为 R2 端口 F0/2 的 IP 地址。

（13）利用 ping 命令测试网络的互通性。

命令参考：

在 PC1 中，输入 C:\>telnet 192.168.2.20

在 PC2 中，输入 C:\>telnet 192.168.2.10

（14）保存 R1、R2 所做的所有配置。

六、实训小结

通过本次实训，你掌握了哪些技能？

实训 11　IP 标准访问控制列表

一、实训目的

1．理解利用 IP 标准访问控制列表对网络流量的控制。

2．掌握如何在路由器上配置 IP 标准访问控制列表。

二、实训背景

假设某公司有三个部门：经理部、财务部和销售部，通过两台路由器连接进行信息传输。为了安全起见，公司领导要求销售部不能访问财务部，但经理部可访问财务部。假设

你是该公司的网络管理员，现要在路由器上做适当配置，实现上述功能。

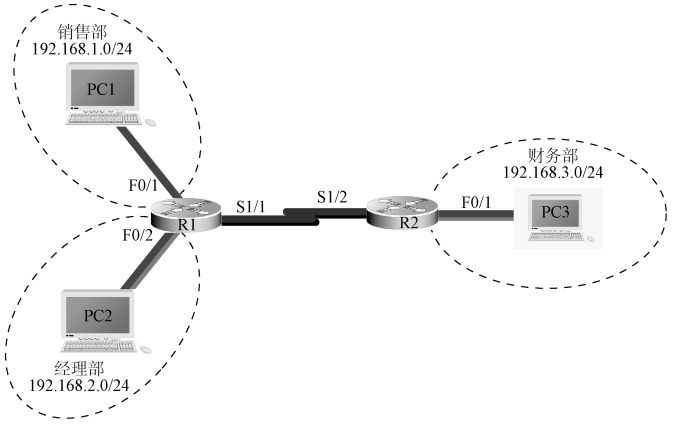
本实训以两台 R2624 路由器为例，分别命名为 R1、R2，通过串口以 V.35 DCE/DTE 电缆连接；通过交叉线分别将销售部 PC1 和 R1 的 F0/1 端口、经理部 PC2 和 R1 的 F0/2、财务部 PC3 和 R2 的 F0/1 端口连接。假设 PC1 的 IP 地址为 192.168.1.10/24，PC2 的 IP 地址为 192.168.2.20/24，PC3 的 IP 地址为 192.168.3.30/24；R1 的 S1/1 端口的 IP 地址为 192.168.4.1/24，F0/1 端口的 IP 地址为 192.168.1.1/24；R2 的 S1/2 端口的 IP 地址为 192.168.4.2/24，F0/1 端口的 IP 地址为 192.168.3.1/24。

三、实训条件

（1）R2624 路由器 2 台。
（2）PC3 台。
（3）V.35 DCE/DTE 电缆 1 根。
（4）交叉线 3 根。
（5）反转线 1 根。

四、实训拓扑

拓扑结构如下图所示。



五、实训过程

（1）认识各线缆、PC 的 COM 端口、路由器各端口和 Console 端口，并按上图连接。

（2）通过一根反转线分别将 R1、R2 的 Console 端口与任意一台 PC 的 COM 端口连接，打开该 PC 的超级终端窗口，进行对 R1、R2 的配置。

（3）分别配置两台路由器的名称：R1、R2。

（4）配置 R1 各接口的 IP 地址和串口（DCE 端）的时钟频率。

命令参考：

```
R1（config）#interface fastethernet 0/1
R1（config-if）#ip address 192.168.1.1 255.255.255.0
R1（config-if）#no shutdown
R1（config）#interface fastethernet 0/2
R1（config-if）#ip address 192.168.2.1 255.255.255.0
R1（config-if）#no shutdown
R1（config）#interface serial 1/1
R1（config-if）#clock rate 64000
R1（config-if）#ip address 192.168.4.1 255.255.255.0
R1（config-if）#no shutdown
```

注意：如果两台路由器通过串口直接互联，则必须在其中一端（DCE 端）设置时钟频率。

（5）验证 R1 接口配置。

命令参考：

```
R1#show ip interface brief
```

（6）配置 R1 的默认路由。

命令参考：

```
R1（config）#router 0.0.0.0 0.0.0.0 192.168.4.2
```

（7）验证 R1 上的默认路由配置。

命令参考：

```
R1#show ip route
```

（8）配置 R2 各接口的 IP 地址。

命令参考：

```
R2（config）#interface fastethernet 0/2
R2（config-if）#ip address 192.168.3.1 255.255.255.0
R2（config-if）#no shutdown
R2（config）#interface serial 1/2
R2（config-if）#ip address 192.168.4.2 255.255.255.0
R2（config-if）#no shutdown
```

注意：DTE 端不需要配置相应路由器接口的时钟频率。

（9）验证 R2 接口配置。

命令参考：

```
R2（config）#R1#show ip interface brief
```

（10）配置 R2 的默认路由。

命令参考：

```
R2（config）#router 0.0.0.0 0.0.0.0 192.168.4.1
```

（11）验证 R2 的默认路由配置。

命令参考：

```
R2#show ip route
```

（12）分别配置 PC1、PC2 和 PC3 的 IP 地址和网关地址。

注意：PC1 的网关地址为 R1 端口 F0/1 的 IP 地址；PC2 的网关地址为 R1 端口 F0/2 的 IP 地址；PC3 的网关地址为 R2 端口 F0/1 的 IP 地址。

（13）利用 ping 命令测试网络的互通性。

命令参考：

在 PC1 中，输入 C:\>telnet 192.168.3.30

在 PC2 中，输入 C:\>telnet 192.168.3.30

（14）在 R2 上配置标准 IP 访问控制列表。

命令参考：

```
R2（config）#access-list 10 deny 192.168.1.0 0.0.0.255
R2（config）#access-list 10 permit 192.168.2.0 0.0.0.255
R2（config）#interface fastethernet 0/1
R2（config-if）#ip access-group 10 out
```

注意：标准控制列表一般应用在尽量靠近目的地址的接口上。

（15）再次利用 ping 命令测试网络的互通性。

命令参考：

在 PC1 中，输入 C:\>telnet 192.168.3.30

在 PC2 中，输入 C:\>telnet 192.168.3.30

（16）查看 R2 当前的配置。

命令参考：

```
R2#show running-config
```

（17）保存 R1、R2 所做的所有配置。

六、实训小结

通过本次实训，你掌握了哪些技能？